

Secure Electronic Court Lodgement

Pilot Project Report

February 2001

Prepared by:

Ron Walker, The NSW Attorney General's Department

Sally Kay, The Law Society of NSW

Richard Weatherley, Galexia

Table of Contents

1	Project Overview.....	4
	1.1 <i>Project Summary</i>	4
	1.2 <i>Project Participants</i>	4
	1.3 <i>Project Structure</i>	4
	1.4 <i>The Project</i>	5
	1.5 <i>Objectives</i>	5
	1.6 <i>Conclusions</i>	6
2	PKI Implementation	8
	2.1 <i>Suppliers</i>	8
	2.2 <i>Issues</i>	9
	2.3 <i>Architecture</i>	12
	2.4 <i>Implementation</i>	13
	2.5 <i>System Deployment</i>	19
	2.6 <i>Problems</i>	20
	2.7 <i>Conclusions</i>	23
3	Issuing digital certificates to solicitors	27
	3.1 <i>Decisions about the architecture of the PKI</i>	27
	3.2 <i>Architecture</i>	28
	3.3 <i>Functions and Responsibilities</i>	29
	3.4 <i>Procedure for Issuance of Certificates</i>	31
4	Electronic lodgement by Solicitors	34
	4.1 <i>Installing the Certificate</i>	34
	4.2 <i>E-Lodgement by Solicitors</i>	35
5	Court Processing.....	40
	5.1 <i>Filing Overview</i>	40
	5.2 <i>Court Processing</i>	41
	5.3 <i>Common Metadata</i>	43
	5.4 <i>Payment Processing</i>	44
	5.5 <i>Document flow</i>	45
6	Appendix – PKI.....	49
	6.1 <i>What is a PKI?</i>	49
	6.2 <i>The Components of a PKI</i>	49
	6.3 <i>PKI Operations</i>	50

6.4	<i>Evaluating a PKI</i>	51
6.5	<i>Secure Messaging</i>	53
6.6	<i>References</i>	54
7	Appendix – Technical Details.....	55
7.1	<i>Baltimore Technologies FormSecure 4.2</i>	55
7.2	<i>Baltimore Technologies FormSecure Toolkit</i>	57
7.3	<i>Database Design</i>	58
8	Glossary	59

1 Project Overview

1.1 Project Summary

This document reviews the Secure Electronic Court Lodgement Pilot Project conducted July/August 2000 undertaken between the NSW Attorney General's Department, the Law Society of NSW and the NSW Land and Environment Court. The project's aim was to pilot an implementation of Public Key Infrastructure (PKI) to aid the secure exchange of documents between the Courts and its customers.

The project delivered a proof of concept of PKI technology and provided a basis for the further refinement of the Attorney General's Department's Electronic Service Delivery (ESD) plan. The project was funded by a grant under the NSW Office of Information Technology *connect.nsw* program.

1.2 Project Participants

1.2.1 Project Group

- * The NSW Attorney General's Department jointly coordinated the project and provided technical services to the Land and Environment Court, including network security configuration. The web server was hosted in a public area of the AGD network known as the De-Militarised Zone (DMZ).
- * The Law Society of NSW jointly coordinated the project. It acted as the Registration Authority (RA) and liaised with customers of the Court (selected solicitors from law firms).
- * The NSW Land and Environment Court pilot trialed the electronic lodgement of Class 4 documents. This required a court administrator to perform appropriate manual tasks when documents were lodged. The pilot was run in parallel with the existing paper-based lodgement system.
- * Solicitors from eight NSW law firms participated as customers and lodged a total of about 50 documents. Participants were issued with digital certificates and certificate storage software from Baltimore, whose Security Domain subsidiary acted as the root Certificate Authority (CA). The participants were able to digitally sign and encrypt Class 4 documents and lodge them with the Land and Environment Court via the Internet.

1.2.2 Technical Assistance

- * Baltimore Technology provided the software and technical expertise in setting up the Public Key Infrastructure and acted as the Certification Authority.
- * Galexia provided the end-to-end solution integration including user interface design, document storage and retrieval, on-line payment processing, server configuration and documentation.

1.3 Project Structure

1.3.1 Project Sponsors

- * Her Honour, Judge Mahla Pearlman – Chief Justice, Land and Environment Court

- * Mr Russell Cox – Director, Finance and Administration, NSW Attorney General’s Department
- * Mr Mark Richardson – Chief Executive Officer, Law Society of NSW

1.3.2 Project Management Group

- * Mr Ron Walker, NSW Attorney General’s Department
Phone: 9228 7019
Email: ron_walker@agd.nsw.gov.au
- * Ms Sally Kay, Law Society of NSW
Phone: 9926 0279
Email: sxk@lawsocnsw.asn.au

1.4 The Project

The pilot comprised three parts:

1. A Public Key Infrastructure (PKI) employed to securely submit documents from solicitors to the Court;
2. Lodgement of documents at the Court via a secure web page; this also included notification to the Court that a document had been received and involved the Court receiving payment; and
3. Receipt of the document by the Court with notification of document receipt sent to the firm that lodged it.

1.5 Objectives

The primary objective of the Pilot was to remove the requirement for Solicitors to physically lodge documents with the Court and for the Court to dispense with, as far as possible, the requirement to keep a physical file of Court documents. The aim was to prove the concept of the secure electronic exchange of documents between the courts, Government and the legal profession. The Broad Objectives related to the establishment, through consultation, of policies and standards relating to the secure electronic exchange of documents. The more specific objectives related to the technical methods of achieving secure electronic exchange.

1.5.1 Broad Objectives

- * Identify court processes requiring re-engineering to exploit secure e-commerce transactions.
- * Identify court processes requiring re-engineering to take advantage of the benefits of electronic lodgement.
- * Allow the Law Society to gain an insight into the requirements of setting up a Public Key Infrastructure for the legal profession that will enable the legal profession to exchange secure documents with clients and government.
- * Dispel fear barriers related to security for the growth of e-commerce within the legal sector.
- * Provide a mechanism for the Attorney General’s Department and the Law Society to define policies and standards for the on-line exchange of data between the legal profession and other Government agencies as well as between Government agencies.

1.5.2 Specific Technical Objectives

At the conclusion of the Pilot the aim was to have:

- * Examined and proved the concept of the use of public key technology by solicitors to lodge court documents.
- * Examined and proved the concept of the electronic lodgment of documents at the Land and Environment Court.
- * Examined and proved the concept of the Land and Environment Court receiving payment with Court documents.

The Pilot was not intended to evaluate or model Court document management systems. This Pilot was a 'Proof of Concept' and is not scaleable to a production system.

1.6 Conclusions

1.6.1 Outcome

The Pilot has answered a number of questions that were posed at the start of the project.

- * Was the pilot a successful proof of getting html forms and/or documents signed digitally?
- * What issues did the pilot highlight with respect to digitally signing messages and/or documents?

The Pilot proved that it was possible for solicitors to digitally sign HTML forms and attached documents, and to securely lodge this information with the Court via the Internet. 25 documents were lodged using the system. It also showed that it was possible for the Court to process these documents, and for solicitors to securely retrieve them.

1.6.2 Public Key Technology

It may be argued that document lodgement does not require the level of security offered by Public Key Technology (PKT):

- * There is no identity check in place for the current manual lodgement system at the Land and Environment Court.
- * It seems unlikely that someone would seek to lodge a false court document, especially if a lodgement fee was due.
- * It may be argued that most Court documents are not sensitive therefore encryption during transmission is not required.

Other requirements in the court process, such as document integrity, confidentiality and non-repudiation can be fulfilled by PKT however there may be more cost effective methods of achieving these requirements. For example, SSL can be used to encrypt documents in transmission, passwords to ensure confidentiality and Adobe Acrobat PDF to ensure document integrity. It was outside the scope of the pilot to examine these options and it is acknowledged by the authors that each of these solutions have limitations.

1.6.3 Court Processes

A simple document management system had to be developed to cater for the storage of documents for this pilot. The pilot did not integrate with the court's case management system.

The pilot demonstrated the concept that electronic lodgements could occur for certain documents without any manual intervention by court staff.

A number of issues were identified but not necessarily resolved:

- The current range of payment options is very narrow and not adaptable to electronic transactions. The pilot proved the concept that payment could be accepted but the method chosen, credit cards is not practical for all court participants and other payment methods need to be explored.
- The ability to lodge documents outside of “court hours” will require review of rules and protocols. The return date/time is currently set for close of business on a day, is this appropriate?
- The service of documents is the responsibility of the party lodging the document. How can this be achieved with documents lodged electronically? The rules will need review to cater for electronic service.

1.6.4 Establishing Public Key Infrastructure

This issue is beyond the scope of the pilot however the objective was for NSW Law Society to gain an insight into the requirements of setting up a Public Key Infrastructure. This project did successfully establish a temporary infrastructure which enabled the secure exchange of documents with solicitors and the court.

2 PKI Implementation

2.1 Suppliers

2.1.1 PKT Vendor

The Law Society of NSW selected Baltimore Technologies as the provider of core public key technology for the pilot project. Baltimore Technologies' products enable full security for data transmissions across the Internet and ensure

- * Confidentiality – provided by the use of triple DES strong encryption;
- * Integrity – provided by the use of Digital Signatures;
- * Authentication – provided by the use of X.509 digital certificates;
- * Proof of a transaction or 'Non-Repudiation' – provided by the use of a Public Key Infrastructure to issue digital certificates.

Baltimore Technologies recommended the use of their FormSecure and MailSecure products in the pilot:

- * FormSecure is a software product that enables public key cryptographic security in web-based HTTP-based form/document submissions between client and server computers. Form data and file attachments entered by end-users into web pages is secured (signed and/or encrypted) before it leaves the end-user's computer, and is desecured once it reaches the server.
- * MailSecure is a software product that enables the full set of security functions to be added to email systems.

Security Domain Pty Ltd, a subsidiary of Baltimore acted as the Certification Authority (CA) for the purposes of the Pilot.

2.1.2 PKI Solution Developer

Galexia was selected to develop the pilot PKI solution, including:

- * Integration of Baltimore Technologies' FormSecure product into an end-to-end web-based document lodgement application, including user interface design
- * Provision of a document repository and the document storage and retrieval interface
- * On-line payment processing software
- * Server configuration
- * Technical documentation

Galexia delivers "best-of-breed" Internet solutions and specialises in security and privacy solutions.

2.2 Issues

2.2.1 *Issuing Private Keys and Certificates*

In principle, certificates could be issued to individual solicitors and/or their firms.

The Security Domain CA issues certificates to individuals, hence individual solicitors were provided with certificates. It was noted that current Court lodgement procedures do not require a solicitor to present proof of identity.

2.2.2 *Multiple Digital Signatures*

Baltimore FormSecure supports “multi-signing”. This means a web page can be digitally signed and/or encrypted by more than one person before being sent on to the transaction server for processing.

It was agreed that documents requiring multi-signing would not be included in the Pilot.

2.2.3 *Document Formats*

A number of factors affected the choice of document formats that could be accepted:

- * Court documents are available in the proprietary Microsoft Word format.
- * Most solicitors use Microsoft Word for authoring court documents, although some solicitors use WordPerfect.
- * It was thought not to be feasible to explain to solicitors how to save documents in open document formats such as RTF. There are incompatibilities and formatting issues in the RTF produced by word processors.
- * It was thought, for the purposes of the Pilot that it was not feasible to require that solicitors lodge documents in Adobe Acrobat (PDF) format as this is proprietary and requires the purchase of additional software.
- * Solicitors must be able to retrieve and view documents on the court file. Hence documents on file must be limited to a minimum set of open and proprietary formats and versions.
- * Microsoft Word 97 and 2000 have same file format so there are no conversion problems
- * It should be possible to lodge document images: eg TIF, JPEG, and GIF formats.
- * Some document formats create larger files than others. Large files are more likely to cause online lodgement to fail.

It was agreed the pilot would accept the following document file formats:

- * PDF
- * RTF
- * TIF
- * JPEG
- * GIF
- * Word 97 or higher

2.2.4 Court Forms

The Land and Environment Court decided that the Pilot would only apply to Class 4 actions, as the Court administration requirements of these documents are relatively simple.

The following documents required the Court to assign a return hearing date:

- * Initiating documents
- * Notices of motion
- * Subpoenas

Some documents also attracted a filing fee. It was decided that the Pilot should include these documents as this would help to identify Court processes requiring change. It was noted that documents where signatures are critical would have to be filed in an image format.

It remained the filing party's responsibility to either print and serve the filed document or advise the other party of an appropriate URL to view and print a copy of the filed document

2.2.5 Exhibits

Exhibits were not included as part of the pilot, as they could:

- * Be quite voluminous (it is not uncommon to receive boxes of documents),
- * Require original documents, or
- * Be something other than a document, eg. a piece of equipment.

2.2.6 Web versus Email Delivery

Web-based forms provide a consistent document lodgement and retrieval interface for users of the system. Documents were filed through a web interface, using a form compatible with Baltimore Technologies' FormSecure product. Completion of a web-based form also allowed the capture of the metadata to a repository.

2.2.7 Payment for Documents Attracting Lodgement Fees

For some Class 4 documents (notably originating process and subpoenas) there was a lodgement fee and a requirement for a court seal. These documents were accepted electronically provided credit card details were included with the metadata. The online payment was tested against a "dummy" credit card clearing system simulating the Remedy Ingenico OCV credit card clearing facilities at Births, Deaths and Marriages. Documents were accepted for lodgement only when this payment simulation was successful. Please note that these types of Class 4 documents were lodged and paid for manually at the Court as usual.

2.2.8 Authentication

Solicitors stored their certificate and keys on their PCs using Baltimore Technologies' key storage software. Their certificates were not stored in their browsers; hence it was not possible for solicitors to use their certificates for authentication when accessing the Attorney General's Department web server. As an alternative the Law Society supplied the participants with a username/password pair for web server authentication. Thus the web server application required a username/password repository.

2.2.9 Lodgement Format

It was a requirement that Class 4 documents should be digitally signed and securely lodged. It was also mandated that multiple documents could be signed and filed in a single electronic lodgement. Upon lodgement the document and associated metadata were added to a document repository. The stakeholders agreed the precise metadata requirements for each type of Class 4 document able to be lodged. There was no requirement for XML-based metadata, as this was not adding value to the FormSecure lodgement process.

One or more applicants and respondents could be involved in a matter, hence the Pilot system had to provide support for multiple solicitors and parties.

2.2.10 Signature Verification

A public key certificate store was required on the server in order to verify the digital signatures attached to filed documents. The Pilot software was designed so that the signature could be verified by using a certificate fingerprint (SHA-1 hash of the DER encoded X.509 certificate) or a certificate stored in an LDAP directory. A Certificate Revocation List (CRL) was not used.

A signed web page was returned to the user upon a successful lodgement.

2.2.11 Email Receipt

Participating solicitors received digitally signed email receipts from the court indicating whether the lodgement was successful. The lodgement web server automatically issued these emails once a document was lodged successfully. It was decided that the web server would generate the official timestamp at the moment the document was received and its digital signature was verified. Documents lodged outside of Court opening hours would be treated as if lodged at the start of the next business day.

The system alerted the Court administrator to new lodgements via an email message and a pop-up dialog box in their web browser. Documents requiring the attention of the Court generated another email to the applicant (and potentially the respondent) when processing was completed.

2.2.12 Email Notification to Other Parties

Along with the email receipt to the applicant, the respondent in the matter received a signed email from the court indicating that a document had been lodged and that it was available for retrieval.

2.2.13 Secure Document Retrieval

Participants were able to retrieve documents from the web site via a username and password over 128-bit server-side SSL/TLS. The document repository included a simple search interface based on matter name and number only. Only solicitors acting for parties to a matter were able to access that court file.

2.2.14 Encryption

It was decided that FormSecure would encrypt documents lodged from the browser to the server using triple DES.

2.2.15 Firewalls

It was decided that the AGD Internet firewall provided adequate security protection against intrusion.

2.3 Architecture

2.3.1 Lodgement

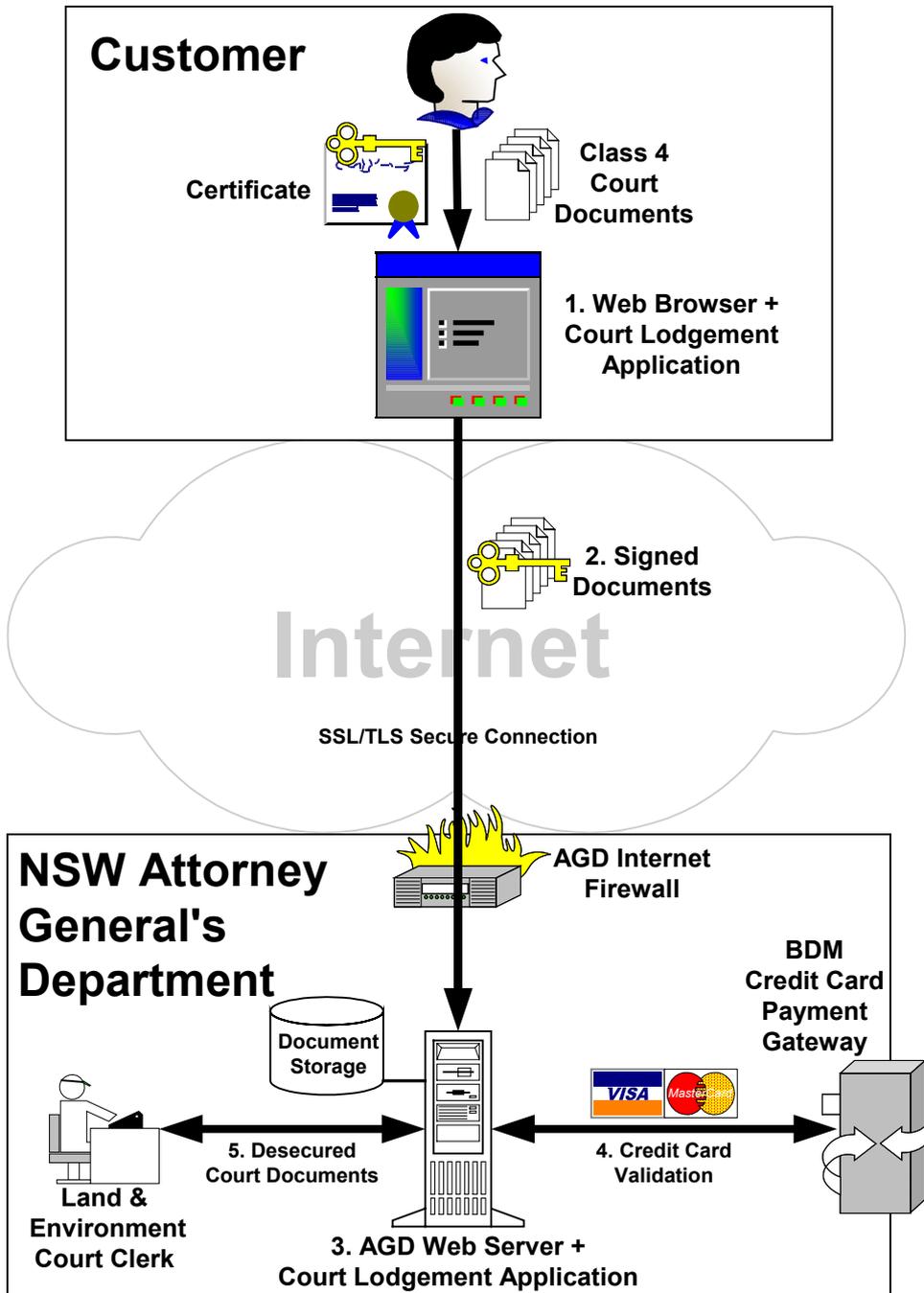


Figure 1 - Secure lodgement of Class 4 Court documents

2.3.2 Notification and Retrieval

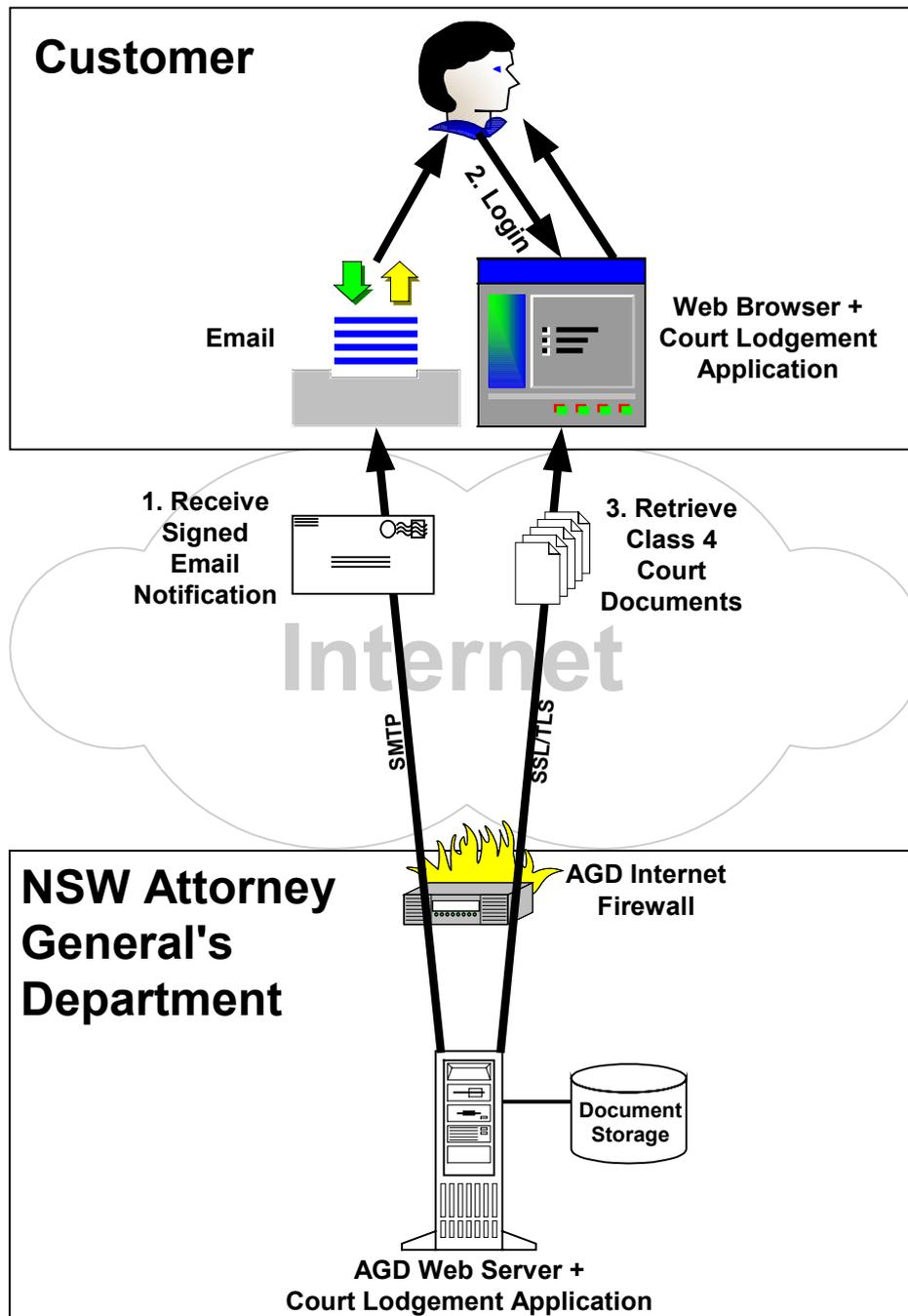


Figure 2 - Signed notification and secure retrieval of documents from Court file

2.4 Implementation

Galexia developed the court lodgement application (dubbed “ELodge”) using state-of-the-art Enterprise Java technology: servlets, JavaServer Pages (JSP), JDBC, the Java Naming and Directory Interface (JNDI), and JavaMail. The metadata and document store was developed using the Informix Cloudscape embedded database. The application (including the database) operates within one Java Virtual Machine instance.

The interface to the Ingenico OCV credit card payment gateway was developed in Java and operates over TCP/IP.

The following sections provide a brief walkthrough of the court lodgement application from the perspective of an end-user.

2.4.1 *Secure Login*

The user is initially presented with a login form asking for username and password authentication. This login is secured using SSL/TLS via a 128-bit “step-up” certificate installed in the web server. User session state is maintained by the use of session-based cookies. There is a 30 minute inactivity timeout, upon which the user is logged out.



2.4.2 *Installation of Client Applet*

When participants first log in to the lodgement application, the client software component downloads automatically and is installed in their web browser. This client applet includes the extensive cryptographic library required to perform signing, encryption, key management etc.

As part of the client software installation, both Netscape and Internet Explorer browsers detect that the software is seeking special privileges. Users are prompted to grant the software these privileges.

Note that the client software library is itself signed, and that it is possible for users to examine the validity of Baltimore Technologies' signing certificate prior to granting the software the special privileges.

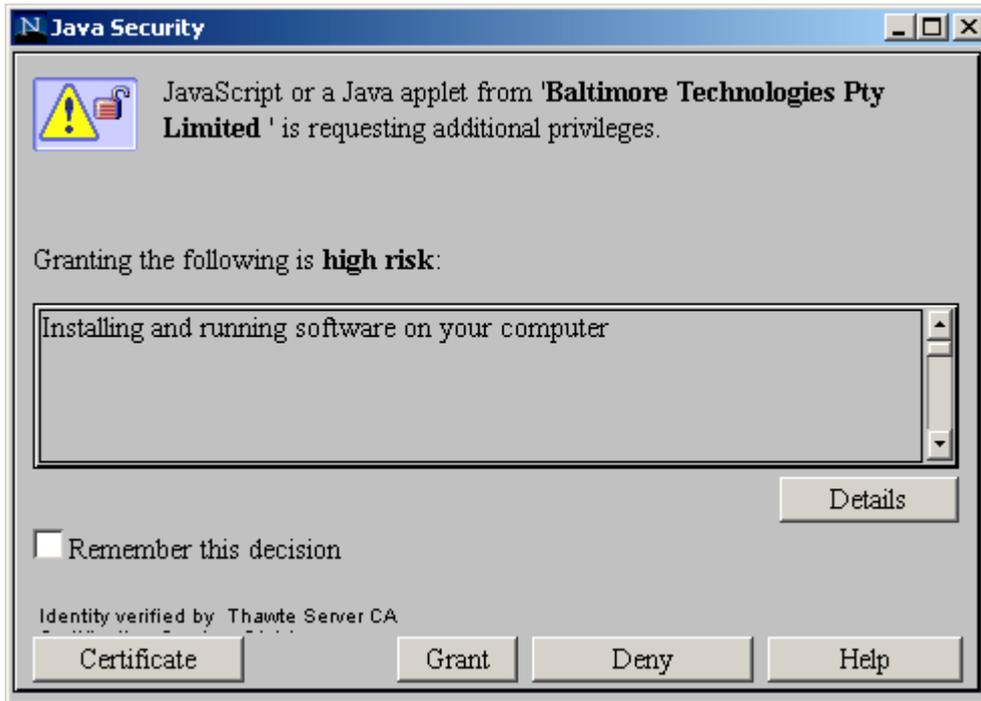


Figure – Client software installation seeking special privileges in Netscape

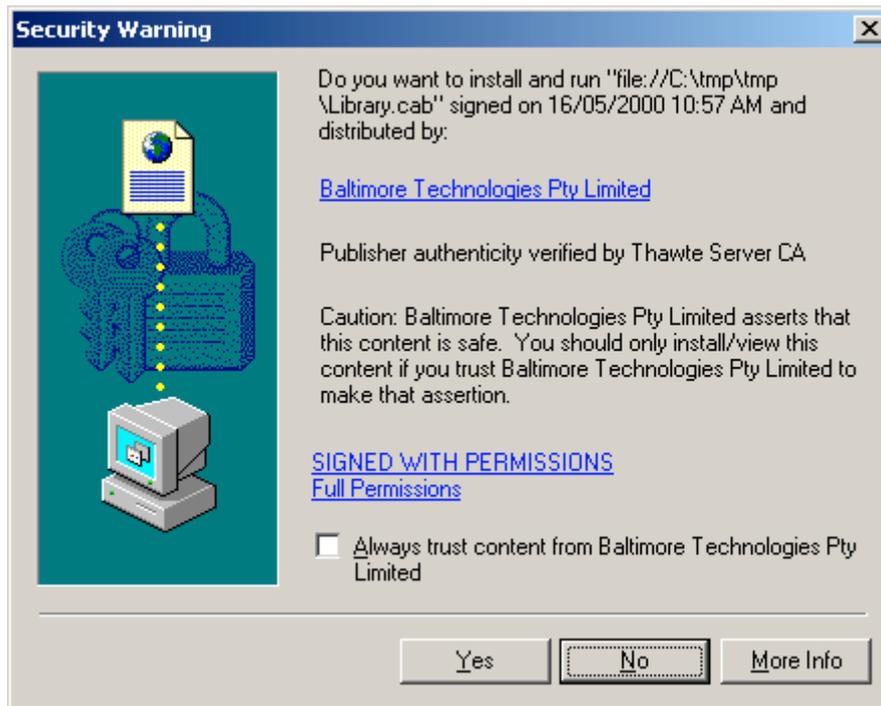


Figure – Client software installation seeking special privileges in Internet Explorer

2.4.3 Installation of MailSecure

At installation time participants are able to optionally install Baltimore Technologies' MailSecure e-mail software. This software was made available by Baltimore so that participants could receive and validate signed email notifications from the Court. MailSecure is compatible with the following popular e-mail client packages:

- * Eudora

- * Lotus Notes
- * Microsoft Outlook

MailSecure also provides its own proprietary mail client.

2.4.4 Lodgement

The solicitor performing a document lodgement is presented with a sequence of three web pages in the format of the popular “Wizard” interface metaphor.

Depending on the metadata entered in the first two Wizard steps, the final data entry page presents a comprehensive set of questions related to applicant, respondent, file(s) to be uploaded, credit card details, and a total cost for the lodgement.

When the user has completed the entry fields, they click on the “Lodge Documents” button to finalise the lodgement.

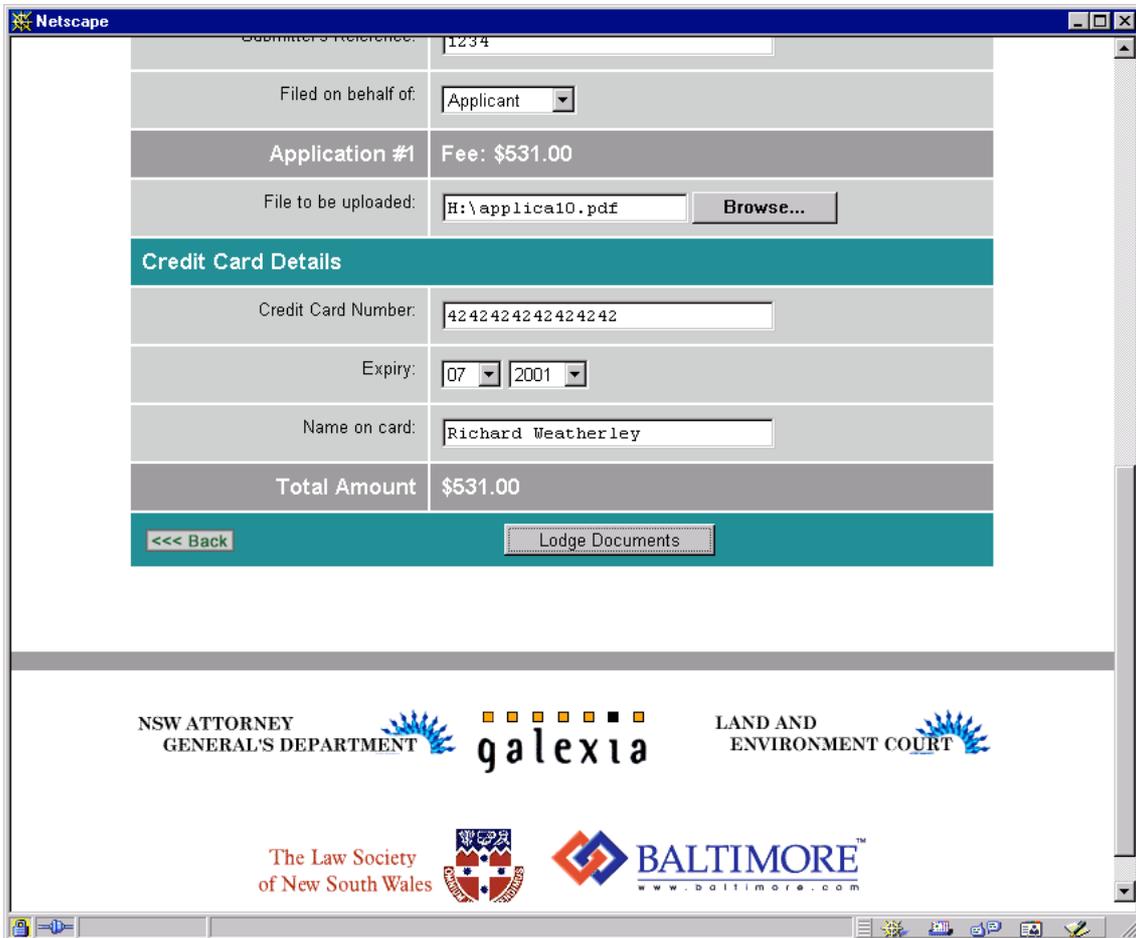


Figure – Third stage of court lodgement “Wizard”

2.4.5 Digital Signing

At this point, the Web browser transfers control to the Baltimore signing applet. This applet displays a popup window asking the user for the passphrase to their keystore held on their PC's hard disk drive.

The user enters their passphrase, allowing the applet to use their private key to sign the entire lodgement. Note that metadata fields and all attached documents are bundled into one digitally signed “package”. This package is then transmitted via HTTP POST to the web server.



Figure – Client applet prompting for the passphrase to the participant’s local keystore

2.4.6 Server Processing

When the digitally signed “package” is received at the web server, it is passed to a Java servlet for processing. The servlet performs several steps:

- * Validation of the digital signature
- * The lodgement timestamp is generated
- * Separation of the metadata from the document(s)
- * Credit card processing occurs (if appropriate)
- * Metadata and document(s) are added to the data store, based on Court filing rules. The original signed lodgement “package” is also stored in the database for auditing purposes.
- * A receipt web page is displayed
- * An email receipt is sent to the participant (digitally signed by the Court)

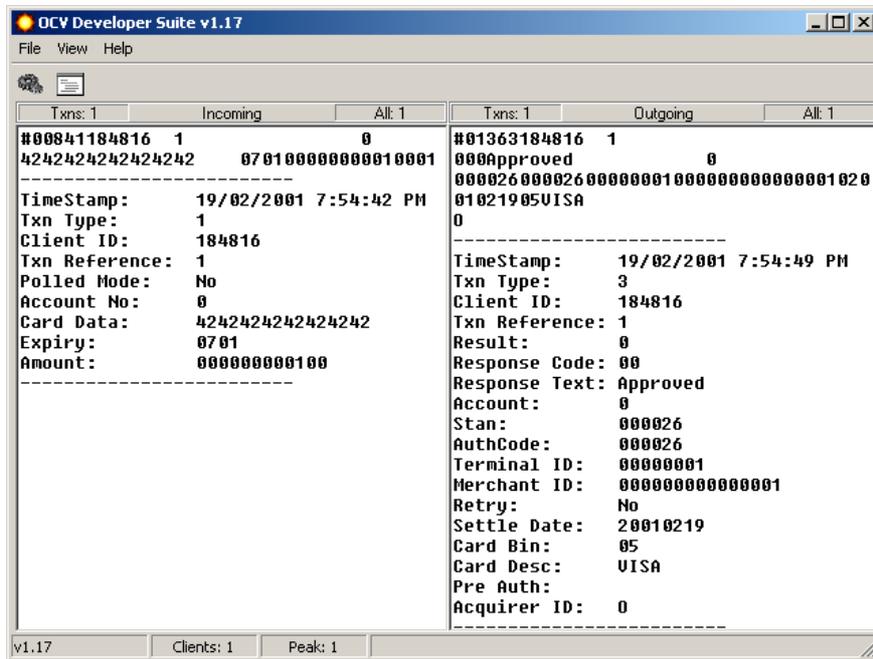


Figure - Ingenico OCV Development Suite (“dummy” credit card validation server)

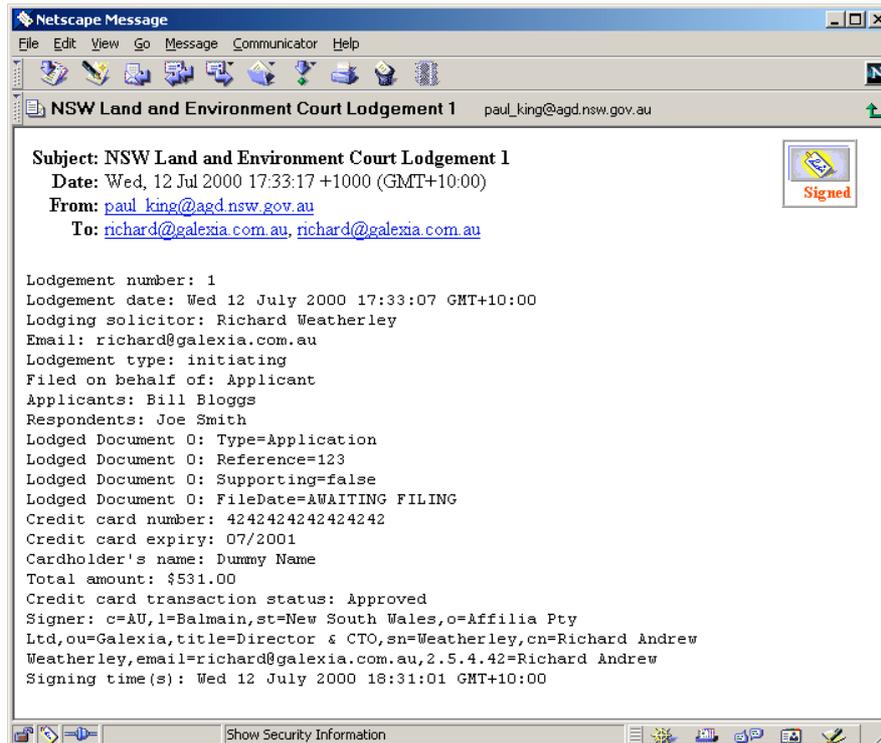


Figure – Signed email notification is received by the participant

The following is the contents of the signed email notification showing the cleartext message and S/MIME Cryptographic Signature attachment.

```
Received: from gimp.agd.nsw.gov.au (pix208a.magna.com.au [203.111.111.208])
  by derrida.galexia.com.au (8.9.3+Sun/8.9.3) with SMTP id RAA26888;
  Wed, 12 Jul 2000 17:31:46 +1000 (EST)
From: paul_king@agd.nsw.gov.au
Received: from ln_gateway.agd.nsw.gov.au by gimp.agd.nsw.gov.au
  via smtpd (for derrida.galexia.com.au [61.8.15.82]) with SMTP; 12 Jul 2000 07:31:47 UT
Received: from gimp.agd.nsw.gov.au ([10.3.11.10]) by mail.agd.nsw.gov.au (Lotus SMTP MTA v4.6.6 (890.1 7-16-1999))
  with SMTP id 4A25691A.0028FD4A; Wed, 12 Jul 2000 17:27:42 +1000
Message-ID: <553678.963387198068.JavaMail.SYSTEM@mail.agd.nsw.gov.au>
Received: from ELODGE by gimp.agd.nsw.gov.au
  via smtpd (for ln_gateway.agd.nsw.gov.au [10.4.11.2]) with SMTP; 12 Jul 2000 07:31:32 UT
Date: Wed, 12 Jul 2000 17:33:17 +1000 (GMT+10:00)
To: richard@galexia.com.au, richard@galexia.com.au
Subject: NSW Land and Environment Court Lodgement 1
Mime-Version: 1.0
Content-Type: multipart/signed; protocol="application/x-pkcs7-signature"; micalg=shal;
  boundary=8373327.963387197878.JavaMail.SYSTEM.elodge
Content-Length: 5675

--8373327.963387197878.JavaMail.SYSTEM.elodge
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit

Lodgement number: 1
Lodgement date: Wed 12 July 2000 17:33:07 GMT+10:00
Lodging solicitor: Richard Weatherley
Email: richard@galexia.com.au
Lodgement type: initiating
Filed on behalf of: Applicant
Applicants: Bill Bloggs
Respondents: Joe Smith
Lodged Document 0: Type=Application
Lodged Document 0: Reference=123
Lodged Document 0: Supporting=false
Lodged Document 0: FileDate=AWAITING FILING
Credit card number: 4242424242424242
Credit card expiry: 07/2001
Cardholder's name: Dummy Name
Total amount: $531.00
Credit card transaction status: Approved
Signer: c=AU,l=Balmain,st=New South Wales,o=Affilia Pty Ltd,ou=Galexia,title=Director & CTO,sn=Weatherley,cn=Richard
Andrew Weatherley,email=richard@galexia.com.au,2.5.4.42=Richard Andrew
Signing time(s): Wed 12 July 2000 18:31:01 GMT+10:00

--8373327.963387197878.JavaMail.SYSTEM.elodge
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"
Content-Description: S/MIME Cryptographic Signature

MIAGCSqGSIB3DQEHAgCAMIACAQExCzAJBgUrDgMCGGUAMIAGCSqGSIB3DQEHAAcAJIAEggnN6Q29u
dGVudC1UeXB0iB0ZXB0L3BsYwluOyBjaGFyc2V0PjVzLWFzY21pDQpDb250ZW50LVRyYW5zZmVy
```


- * Sun JavaBeans Activation Framework 1.0.1
- * Sun JavaMail 1.1.3
- * Galexia ELodge application (including Galexia E-Business Suite)
- * Optional: Ingenico OCV Development Suite (credit card validation server). NOTE: this only runs on Windows NT 4.0 SP5 or Windows 2000 SP1.

2.5.3 *Internet Client*

The following software was required on the participants' PCs:

- * Windows 95/98/NT/2000 Pentium class PC with minimum 64MB memory
- * Netscape Navigator/Communicator 4.5+ or Microsoft Internet Explorer 4+ with support enabled for Java, JavaScript and cookies. Ideally the browser should support step-up 128-bit SSL connections (strong encryption). NOTE: The US has lifted export restrictions on 128-bit secure versions of Netscape and Internet Explorer.
- * Optional: Email client that supports S/MIME email signed with 128-bit certificates,
- * Optional (for court administration): Adobe Acrobat 4.0

NOTE: The FormSecure client applets were tested on Apple Mac, UNIX or any other non-Win32 platform. Baltimore Technologies advised that the FormSecure applets will not operate correctly on these platforms.

2.5.4 *SSL Web Server Certificate*

A 128-bit step-up SSL certificate was installed in the iPlanet web server to enable encrypted lodgement and document retrieval. A backup copy of the certificate was held in a secure place, along with its passphrase.

2.5.5 *Public Keys of Participants*

The fingerprints file was installed on the production server. This file contained a list of fingerprints (an SHA-1 hash of the DER encoded X.509 certificate) for each participant. NOTE: These certificates must be valid and issued by a recognised root CA. Each line in the file was either a hex fingerprint or a comment (starting with a '#' character). Eg.

```
# Certificate fingerprints for participants in LEC lodgement pilot project
#
# Solicitors
# -----
# Joe Bloggs joe.bloggs@somelawfirm.com.au
0106008E236BF966EC464ED4736823A681613C4E
```

2.5.6 *Court Signing Key*

The NSW Land and Environment Court were issued with a signing certificate that was used to sign the email acknowledgment messages sent from the Court. This keystore was installed on the server and file permissions were set to read only for Administrator (on NT) or root (on Solaris), and deny access to all other users.

2.6 **Problems**

Galexia encountered a number of significant technical problems with Baltimore Technologies FormSecure product. These problems introduced delays and increased the development effort.

2.6.1 FormSecure 4.1 Problems

During development and testing, Galexia discovered that FormSecure version 4.1 was unable to accept secure signed uploads containing more than 64KB of information. Thus FormSecure was unusable for the pilot project for any purposes other than simple demonstrations. Baltimore indicated that version 4.2 fixed this problem hence Galexia upgraded the development platform to FormSecure 4.2 and redesigned the lodgement interface forms and server software to integrate with the new version.

2.6.2 FormSecure 4.2 Problems

After migrating to FormSecure version 4.2, Galexia discovered that the product would not work with web-based server applications, such as those built with standard technology like Microsoft ASP (Active Server Pages), Allaire Cold Fusion or JSP (JavaServer Pages). The court lodgement application was built using JSP, so Galexia was unable to proceed with the project using FormSecure. Baltimore indicated that FormSecure would support this requirement in a future version but that this was not available. They suggested utilising a new product – the FormSecure Toolkit – in place of the standard FormSecure product. Galexia upgraded the interface and redeveloped and tested the server software to integrate with the new toolkit.

2.6.3 FormSecure 4.2 Toolkit Problems

The Baltimore FormSecure 4.2 Toolkit 1.0.0 was a 100% pure Java set of security class libraries. The toolkit was tested with Windows NT/2000 and Solaris. A known bug resulted in limited support on non-Win32 platforms. On Solaris, the toolkit only worked when installed in a stand-alone ServletExec Application Server environment (due to file write permission problems when decrypting lodgement messages).

Galexia discovered that the FormSecure 4.2 Toolkit had unacceptable performance characteristics. For example, lodgement of a 100KB file required about 2 minutes of server processing with the CPU at 100% utilisation. Clearly this was an unacceptable wait for users. Baltimore subsequently supplied Galexia with a software patch that provided greatly improved performance.

The signing applet supplied with FormSecure Toolkit did not support encryption. A fundamental requirement of the pilot was that the lodgement is secure during transmission. Baltimore suggested that AGD purchase an SSL web server certificate from Thawte Consulting as an alternative way of providing strong encryption during data transmission. This certificate enabled a “step-up” from 40- or 56-bits to 128-bit encryption for browsers installed prior to the revised U.S. Encryption Export Control Regulations¹.

The signing applet also incorrectly inserted extra blank lines at the head of the first part of the multipart MIME data stream that was sent to the server.

2.6.4 Baltimore Cryptographic Library Instability

Solicitors experienced intermittent lodgement problems due to a bug in Baltimore’s client cryptographic libraries. The bug appeared when files of a certain size were lodged, resulting in rejection of the lodgement. Baltimore could not replicate the problem and the Pilot continued despite this on-going technical problem.

¹ http://www.epic.org/crypto/export_controls/regs_1_00.html

2.6.5 *Poor Certificate Search Facility*

The Security Domain CA Certificate Search facility was unreliable. It was not possible to retrieve the public key certificates for many of the participants through this web interface. Galexia had to directly contact Security Domain several times in order to retrieve all the certificates. The Certificate Search facility consistently caused Netscape Communicator to crash.

2.6.6 *Internet Explorer 5.x Problems*

Various versions of Microsoft Internet Explorer 5.x contain bugs. These include incorrect interpretation of HTTP caching directives, inconsistent operation of Microsoft-specific HTML tags, and inconsistent handling of HTTP content type headers. This resulted in severe, unexpected and inconsistent behaviour when retrieving web pages, applets and different file types from the web server using IE 5.x.

2.6.7 *Additional Performance Issues*

There were several major performance issues (in addition to the performance problems with Baltimore FormSecure):

- * The size of the client cryptographic software libraries and applets was 700KB for Netscape Communicator and 451KB for Microsoft Internet Explorer.
- * Some of the documents transmitted to the server were very large, and increased further in size due to signing and encryption.
- * The bandwidth limitations of dial-up users further decreased the performance of the application.

2.6.8 *Browser and E-mail Support for Security Domain CA*

Popular browsers and e-mail clients did not automatically trust the Root CA of the certificates issued for the Pilot, hence signatures attached to email from the Court could not be validated.

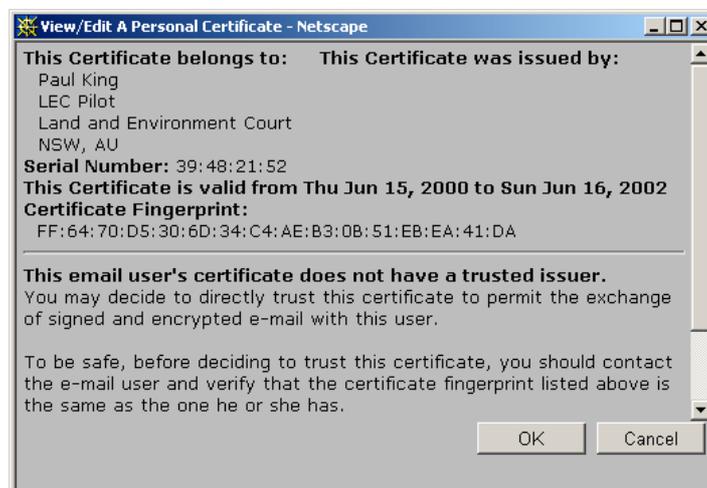


Figure – The issuer of this signing certificate is not trusted by the browser

2.6.9 *Performance*

The participant was forced to wait for a significant period of time from the moment they entered their passphrase to the moment a receipt web page was displayed. This includes:

- * The digital signing of the “package” in the client browser
- * The data transmission from the browser to the server (over encrypted SSL/TLS)

- * The subsequent server processing

The poor overall performance was due to a combination of:

- * Digital signature software in the browser
- * SSL/TLS encryption between the browser and the server
- * Server-side signature verification

2.7 Conclusions

2.7.1 Privacy

Privacy issues were not considered as part of the Pilot. There are specific privacy implications for end users of PKI applications:

- * Collection, use, disclosure, storage and destruction of personal information by Certification Authorities, Registration Authorities and Relying Parties.
- * Certificate revocation lists: wrongful certificate revocation or logging end user activities.
- * Cooperation with law enforcement agencies
- * Access and correction rights for end users over their personal information.
- * Security risks, including compromise of an individual's private key, breaches of security at the Certification Authority or Relying Party etc.
- * Tracking individuals where the certificate is used for more than one purpose.
- * Limits on user choice of certificates and Certification Authorities.

2.7.2 Certificate Expiry and Key History

In a PKI, an end user's certificate commonly includes an expiry date. These certificates are valid for a nominated period only, and typically expire after one year for the following reasons:

- * To minimise the chance of the key pair being compromised.
- * To ensure the key pair remains cryptographically sound (of sufficient key length that it is not in danger of cryptanalytic attack).

This raises a number of practical issues:

- * Certificate renewal/update – this should occur once 70-80% of the key lifetime has been exhausted. It may involve significant management effort to keep certificates up to date.
- * Expired authentication and encryption keys – these keys may still be required to access historical data. Key history can be stored by the end-user or by a trusted third party (such as a CA).
- * Expired signing keys – these keys are typically stored in a key archive. A key archive is a service provided by a trusted third party that can be used for auditing and dispute resolution.

2.7.3 *Key Storage, Backup and Recovery*

Keys and certificates can be stored in software (using a file-based keystore) or hardware (such as a smart card or USB token). A roaming user may not always be carrying a notebook computer or PDA; hence there must be some other method for the user to carry their digital certificates.

It is possible to implement a key backup and recovery facility either as part of a CA or another trusted third party. This is specifically designed for the recovery of encryption keys in situations of forgotten passphrase, corrupted disk (for software-based keystores), lost or damaged hardware token, or due to employee dismissal.

Note that private keys designated for digital signature purposes in support of non-repudiation should never be backed up by a third party.

2.7.4 *File Formats and XML*

Court documents are almost universally authored in word processors – in most instances this is Microsoft Word. Solicitors may be reluctant to produce Court documents using online forms and ‘form-filler’ software made available by the Courts². It may be possible for the Courts to distribute Court document templates for Microsoft Word (and perhaps Word Perfect). There are (at least) five ways that a Court document in Word format may be transferred to the Court file:

- * Without change – any format changes will occur at the Court. It is possible that the Court will convert the document into PDF, attach a seal image, then sign and lock the PDF file. It may also be desirable to sign the Word document at the client, using a commercial product such as CIC Sign-It, DocuTouch, Assured Office, or onSign (free).
- * Conversion from Word format to PDF format at the client, and (optionally) digitally signed at the client, before being filed. This requires each solicitor to obtain and use a copy of Adobe Acrobat.
- * Conversion from Word format to RTF format at the client. Assuming that the document is based on a template, it should be possible for the Court to convert the filed RTF document into any format, including XML, PDF and HTML, and to store the document in a flexible manner.
- * Wrapping the Word, PDF or RTF document(s) in XML using a structure such as defined in the Electronic Court Filing Proposed Standard as proposed by Legal XML³. This standardises the metadata and provides a framework for digital signing.
- * Conversion from Word format to XML at the client. This assumes that the document is based on a template and that Word is capable of cleanly converting to XML. The XML can be digitally signed and transferred to the Court (using a structure such as the Electronic Court Filing Proposed Standard) for flexible storage and retrieval.

Many lodgements include documents and diagrams that are not in digital form. A standard solution for lodging these documents is to scan and attach or embed them as TIFF images.

2.7.5 *Online Payments*

The Pilot demonstrated that fees can be built into the lodgement application and can be processed at the same time as the metadata and documents. A more robust approach is to:

- * Pre-authorise the payment: pre-authorisation is used to make sure that the card is valid and has sufficient credit limit. The pre-authorisation amount is reserved from the user’s credit limit for a short period. The amount is not charged to the credit card account.

² An example (almost) online form application is the ATO TFN Declaration form (using JetForm filler)

³ <http://www.legalxml.org/>

- * Complete the data storage
- * Complete the pre-authorisation
- * Send the signed email notification and receipt

2.7.6 Authentication

Authentication is required to allow solicitors to gain access to the online Court lodgement application. Users can be authenticated using traditional username/password, a one-time password token, a challenge-response token, a mag-stripe card, a digital certificate (possibly stored in software or on a hardware token/smartcard), or using biometric means.

Each of these authentication methods has advantages and disadvantages. For example, in a scheme where a password or passphrase is required, a password retrieval service would be a significant administrative function.

Note that regardless of the authentication technology, the Court will be required to maintain authorisation information for each user, such as which Court matters a particular solicitor is able to retrieve.

For a web-based Court lodgement system using PKT, a user can install their certificate in their browser and instruct the browser to automatically authenticate them when they lodge or retrieve a document. Also note that it is possible to store certificates on a hardware token (such as a USB device) and for this to be “plugged in” to the browser for authentication (or signing or other functions) as required. This is a popular solution for “roaming” users.

2.7.7 Database

It should be noted that a production Court filing system would use a Case Management System as its database for storing documents.

2.7.8 Receipt

The most robust electronic Court receipt is an email message that has been digitally signed by the Court. Many popular email packages (such as Outlook and Netscape) allow the user to verify the signature. These packages implicitly trust a number of CAs. The Court should ensure that their signing certificate should be issued by one of these trusted CAs.

2.7.9 Notification of Parties

In a production system where parties are notified by email of changes to the Court file, it will be critical to ensure that email addresses are up-to-date and that email services are operating on a 24x7 basis.

2.7.10 Certificate Formats

PGP certificates have been widely adopted as an alternative to X.509 Version 3 certificates, especially in non-commercial environments. However, corporate demand has overwhelmingly been in favour of X.509v3 public-key certificates. The vast majority of PKI vendors support only X.509-based certificates.

2.7.11 Multiple signatures, multiple documents

In the Pilot, the lodgement “payload” was signed rather than each document. The FormSecure Toolkit software was unable to handle multiple signatures, and was unable to accept digital signatures from solicitors’ clients. This is an important issue to resolve in a production system. Possible solution include:

- * More advanced versions of FormSecure (or equivalent from other PKI vendors)
- * Proprietary browser plug-ins that support multiple signing

- * A custom XML client application that implements, for example, the Electronic Court Filing Proposed Standard as proposed by Legal XML.

2.7.12 Browser-based lodgement

The Pilot clearly indicated that “thin-client” public key technology is a “work-in-progress”. Browser-based signing applications fall into two or three camps:

- * Java-based software, such as Baltimore Technologies’ FormSecure, which requires close to “zero install” for the end-user. The advantage of this software is that (in theory) it can be used from any computer connected to the Internet, and that it requires minimal technical administration. This is not entirely true of FormSecure – the software was also found to be unstable.
- * Browser plug-ins, such as from PureEdge Solutions’ Internet Commerce System, requires users first download a proprietary plug-in onto their computers. Once they complete this step, they can download and read forms that require this proprietary plug-in. The problem with this approach, aside from having to find and wait for the plug-in to download and install, is that users must also download the forms, a process that can burden them with lengthy waits.
- * Hybrid solutions, such as Jetform Corporation’s ReachForms that utilise HTML, DHTML and/or Java depending on the capabilities of the user’s browser.

A long-term solution needs to consider where and how Court lodgement and retrieval may occur. For example, the FormSecure client platform was limited to Windows 95/98/NT/2000. This excludes:

- * Apple Macintosh users
- * The growing wireless Internet market – PDAs and mobile phones

2.7.13 CP and CPS

The final issue is whether a prospective PKI really addresses the issues of security, obligations of all parties, and liability in case of dispute. This is the role of the Certificate Policy (CP) and Certification Practices Statement (CPS). As a minimum, the following stakeholders should be involved in the drafting of a CP and CPS:

- * PKI Owner
- * Legal staff
- * Security staff
- * IT Department
- * PKI Vendor

The CP or CPS should contain:

- * General Provisions, such as liability, obligations, financial responsibility, interpretation and enforcement, fee, confidentiality and IP rights.
- * Identification and Authentication, including initial registration, routine rekey, rekey after revocation, and revocation request.
- * Operational Requirements, including certificate application, issuance, acceptance, suspension and revocation.
- * Physical and Technical Security Controls.
- * Certificate and CRL Formats.

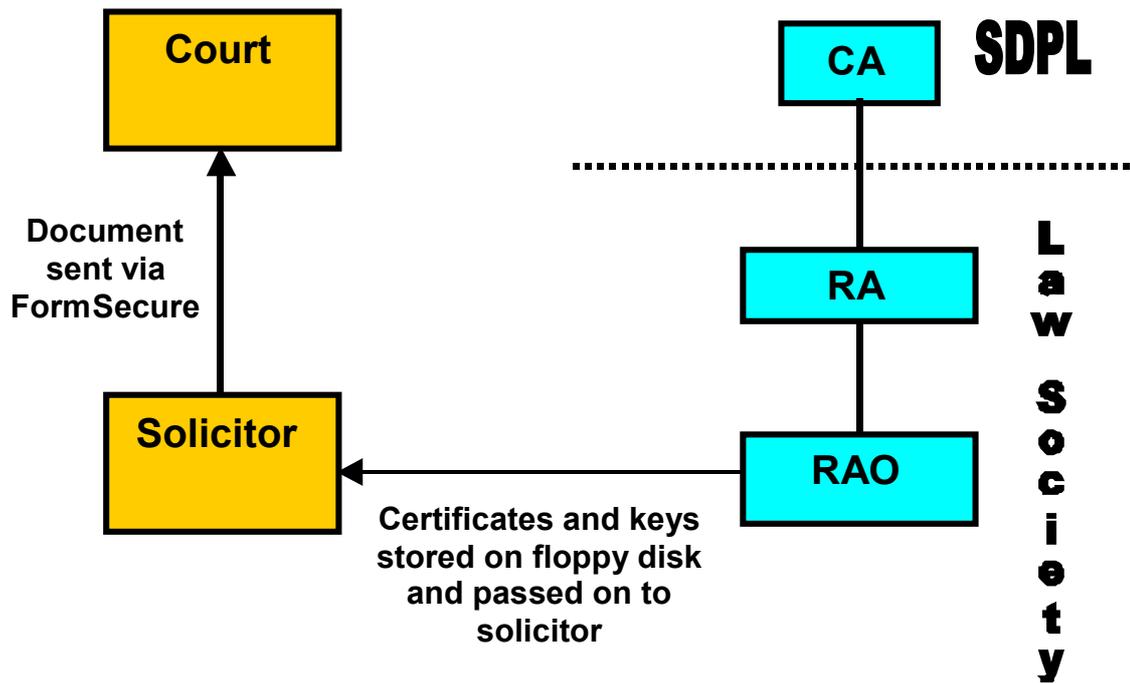
3 Issuing digital certificates to solicitors

3.1 Decisions about the architecture of the PKI

It was decided that Security Domain Pty Ltd, (SDPL), a subsidiary of Baltimore Technology would act as the Certification Authority (CA) and the Law Society would act as the Registration Authority (RA). The Law Society would generate certificates for the Pilot Group and the Land and Environment Court. It was decided that the certificates would be issued to the Pilot Group on a floppy disk after a face to face interview.

3.2 Architecture

3.2.1



3.3 Functions and Responsibilities

3.3.1 Certification Authority (CA) : Security Domain Pty Ltd

Generate Certificates upon receipt of an authorised and validated request for new Certificates or renewal of Certificates from the Law Society. Generation involves:

1. receipt of an approved and verified Certificate request;
2. creating a new Certificate;
3. binding the Key Pair associated with the Certificate to a Certificate owner;
4. issuing the Certificate and the associated public key for operational use.

Generation is performed in a physically secure facility, on the receipt of a properly authorised digital Certificate request.

3.3.2 Registration Authority (RA): Law Society of NSW

1. Generate keys for the project participants
2. Submit the Law Society's public key together with digitally signed certification requests to the CA;
3. Operate the RA in an efficient and trustworthy manner and in accordance with Policies.⁴
4. Register End Users which involves:
 - authenticating material Certificate information, such as sighting Proof of Identity (POI) documentation;
 - proposing and approving distinguished names for Certificate applicants;
 - generating key pairs for Certificate applicants

⁴ The Policies involved are:

- SDPL Certificate Management Policy
- the CA-RA agreement
- documented operational procedures
- the Law Society's internal security and privacy policies;

5. Submit End User public keys together with digitally signed certification requests to the CA, and receive the Certificates issued in accordance with these requests;
6. Issue keys and Certificates to End Users, ensuring that private keys are not obtained by third parties prior to being received by the End User, and that private keys are not captured by any other mechanism under the control of the RA;
7. Authenticate requests from end users for the renewal or revocation of their Certificates, and generate digitally signed renewal or revocation requests to the CA;⁵
8. Make reasonable inquiry to determine the validity of compromises and suspected compromises of private keys at any subordinate level they deem warranted in its chain of trust;
9. Revoke Certificates on receipt of authenticated digitally signed revocation requests, or when their inquiries into the compromise or suspected compromise of a private key have established the validity of a revocation request;
10. Maintain a list of compromised keys and compromised users and periodically provide these lists to their superior CA;
11. Conduct regular internal security audits;
12. Assist in audits conducted by the CA to validate the renewal of their own Certificates.

3.3.3 *End Users*

There were re two End Users for the purpose of this trial:

1. Solicitors
2. The Land and Environment Court

For the purposes of this Pilot, End Users discharged their obligations by:

1. providing the RA with true and correct information at all times;
2. providing sufficient proof of material Certificate information to meet user registration or Certificate renewal requirements;
3. requesting generation of End User keys or requesting acceptance of self generated keys;
4. ensuring that their passphrase is kept safe at all times

⁵ It is unlikely, for the purposes of the Pilot, that functions 7 - 12 inclusive would be used.

3.4 Procedure for Issuance of Certificates

Sally Kay of the Law Society acted as the ‘authorised registrar’ (the Registrar) for the purposes of the Pilot. It was decided to use the highest level of security available, so the Registrar generated keys after a face to face interview with the End User. The process was as follows:

1. The End User personally attended a registration interview, during which the Registrar:
 - obtained the End User’s registration details and Certificate information (that is, the User’s full name, firm and firm address and email address);
 - authenticated the End User’s identity by checking photo identification
 - checked the Law Society’s membership database to ensure that the End User was a solicitor with a current practising certificate.
 - explained the user’s responsibilities attached to possession and use of their public keys and Certificates
2. The RA then generated the Certificate key pairs. This was done using software loaded on a server kept in a secure place in the Law Society. The process the Registrar followed using the software was as follows.

After logging onto the RA system, the following options are presented:



After clicking on “Register a New User” the Registrar then enters the details about the solicitor in a screen as follows:

The screenshot shows a dialog box titled "S. Mongan" with the following fields and options:

- Common Name:** S. Mongan
- Org Unit:** Development
- Organisation:** Baltimore Technologies
- Country Code:** IE
- Finger Print (MD5):** A field containing a series of 'x' characters representing a fingerprint.
- Delivery Mechanisms:** A list with "Send E-Mail Reminder" and "Send Certificate" (selected).
- Certificate warning(days):** 7
- Delivery Mode:** A list with "Auto Roll Certificate" (selected) and "RAD Roll Certificate".
- E-Mail warning(days):** 14

Buttons at the bottom: ACCEPT, REJECT, CANCEL.

Once the details have been entered, keys were generated in PKCS#12 format. The solicitor then enters a passphrase directly into the system.

The screenshot shows a dialog box titled "Set Passphrase (minimum 8 characters)". It contains:

- A small icon of a floppy disk.
- Enter Passphrase:** A text input field.
- Confirm Passphrase:** A text input field.
- Buttons: OK, Cancel.

This passphrase was a minimum of 8 characters with at least one alpha, one numeric, one upper case, one lower case and one special character. No record of the End User's passphrase was recorded by the RA.

3. The Registrar processed the End User's Certificate application and submitted a Certificate request to the issuing CA for each public key, together with the public keys;
4. The issuing CA receives the Certificate requests and keys. On the day of receipt the CA verifies each request, generates and signs the requested Certificates, then:
 - posts the Certificates to the SDPL X.500 Directory;
 - issues the Certificates to the RA;
5. The End User's keys and certificate were given to them on a floppy disk

3.4.1 Problems/Issues

No problems were encountered in administering the Registration Authority. Baltimore's software was intuitive and quick and simple to use.

4 Electronic lodgement by Solicitors

The solicitors accessed the “e-lodge” application through the secure site (<http://www.elodge.agd.nsw.gov.au>). The first step, after logging in, was to import the keys and certificates into the e-lodge application.

4.1 Installing the Certificate

Solicitor imports the keys and Certificates into the elodge application.

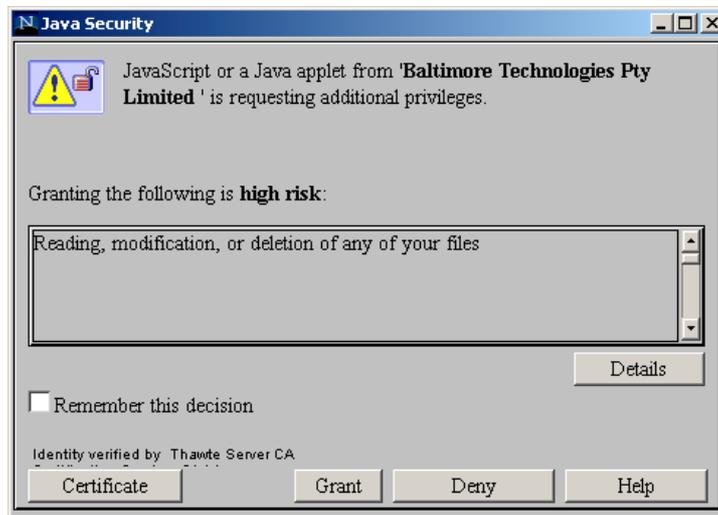


Figure – Browser seeking permission to create the keystore on the solicitor’s PC

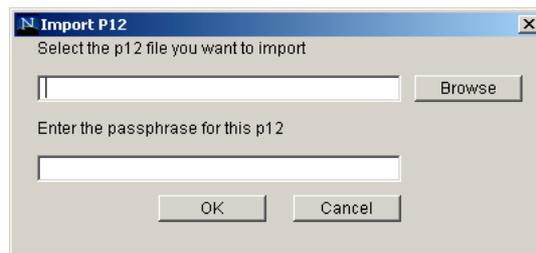


Figure – Admin applet asking for the name and passphrase of the PKCS#12 file to import

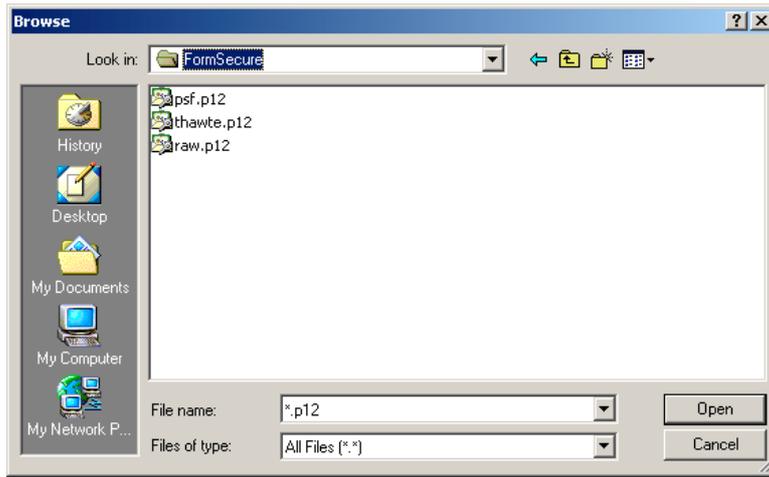


Figure – Solicitor chooses the PKCS#12 file to import

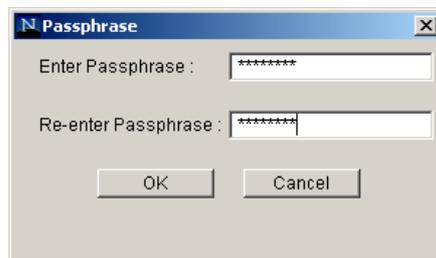


Figure – Solicitor chooses passphrase on new keystore (located on PC hard disk)

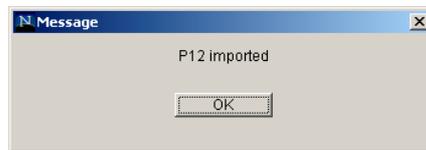


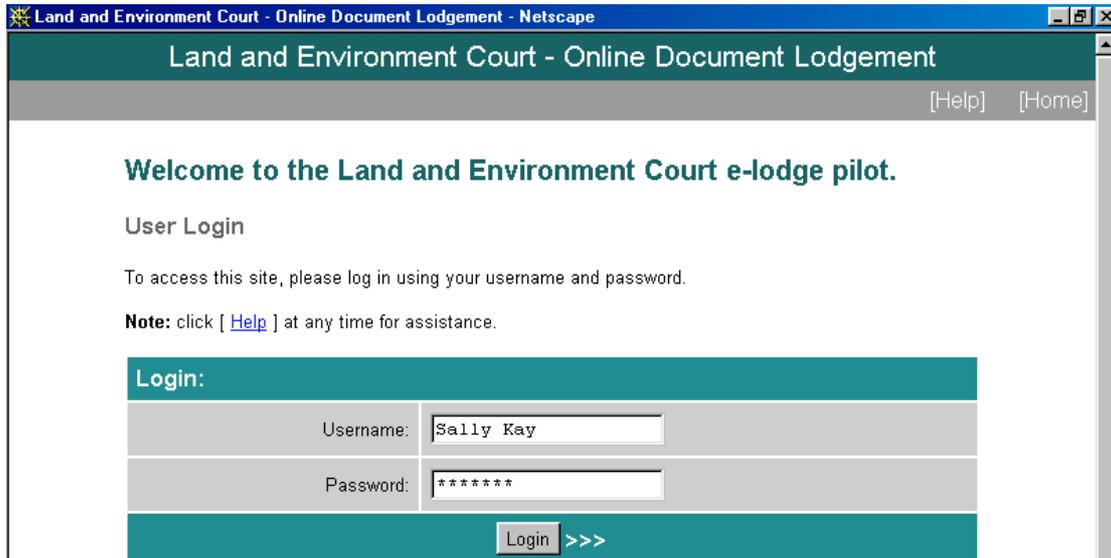
Figure – Import completed

- The End User's keys and Certificates are now ready for operational use.

4.2 E-Lodgement by Solicitors

4.2.1 Logging onto the website

The solicitor goes into the e-lodge website (<http://elodge.agd.nsw.gov.au/>) and logs in using their full name and a password.

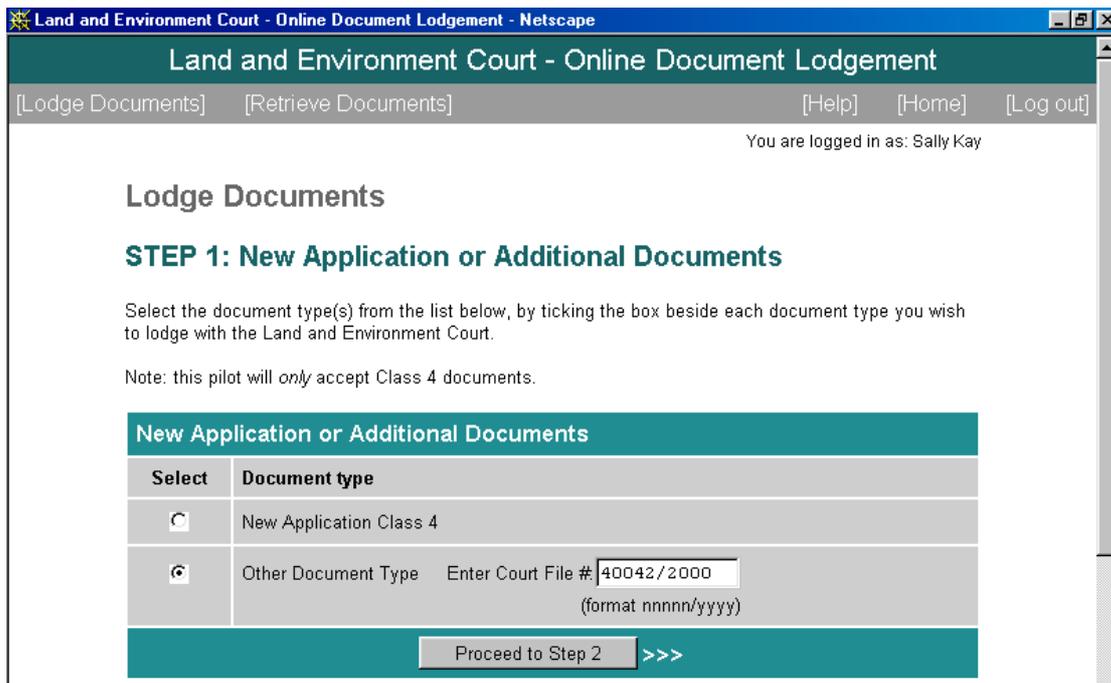


The solicitor then has the option of either lodging or retrieving documents.

4.2.2 Lodging documents

This is a 3-step process:

Step 1: selecting whether the document to be lodged is a new application or a document on an existing matter:



Step 2: The solicitor selects the type of document or documents they wish to lodge

Land and Environment Court - Online Document Lodgement - Netscape

Court File Number: 40042/2000
Enter Number of Documents to Lodge for each Type

Number of Docs	For: Document Type
<input type="text" value="1"/>	Affidavit
<input type="text" value="0"/>	Applicants Points of Claim
<input type="text" value="0"/>	Notice of Appearance
<input type="text" value="1"/>	Notice of Discontinuance
<input type="text" value="0"/>	Notice of Motion
<input type="text" value="0"/>	Notice to Produce
<input type="text" value="0"/>	Respondents Points of Defence
<input type="text" value="0"/>	Subpoena for Production
<input type="text" value="0"/>	Subpoena for Production and to Give Evidence
<input type="text" value="0"/>	Subpoena to Give Evidence

<<< Back Proceed to Step 3 >>>

Step 3: uploading the Word document(s) to be filed:

Land and Environment Court - Online Document Lodgement

[Lodge Documents] [Retrieve Documents] [Help] [Home] [Log out]

You are logged in as: Sally Kay

Lodge Documents

STEP 3: Select files to lodge

Court File Number: 40042/2000

Affidavit #1	Fee: \$0.00
File to be uploaded:	<input type="text"/> <input type="button" value="Browse..."/>
Notice of Discontinuance #1	Fee: \$0.00
File to be uploaded:	<input type="text"/> <input type="button" value="Browse..."/>

<<< Back

If the document is the initiating process, the following screen will open:

Lodge Documents

STEP 3: Select files to lodge

Enter Applicant and Respondent Details

Applicant 1:	<input type="text" value="John Smith"/>
Respondent 1:	<input type="text" value="Lane Cove Council"/>
Solicitor on record:	Sally Kay
Firm Name:	The Law Society of NSW
Firm Address: 1	Level 6
Firm Address: 2	170 Phillip Street
Firm Address: City	Sydney
Firm Address: Postcode	2000
Firm Phone:	02 9926 0279
Firm Fax:	02 9926 0399
Contact Email:	sxk@lawsocnsw.asn.au
Firm DX:	0
Submitter's Reference:	<input type="text"/>
Filed on behalf of:	<input type="text" value="Applicant"/>
Application #1	Fee: \$531.00
File to be uploaded:	<input type="text"/> <input type="button" value="Browse..."/>

Credit Card Details

Credit Card Number:	<input type="text" value="4242424242424242"/>
Expiry:	<input type="text" value="07"/> <input type="text" value="2001"/>
Name on card:	<input type="text" value="Dummy Name"/>
Total Amount	\$531.00

4.2.3 Signing the package

Land and Environment Court - Online Document Lodgement

[Lodge Documents] [Retrieve Documents] [Help] [Home] [Log out]

You are logged in as: Sally Kay

Lodge Documents

STEP 3: Select files to lodge

Court File Number: 40042/2000

File

Notice of Discontinuance

File to be uploaded: J:\Backups\Members Ser

<<< Back

Lodge Documents

4.2.4 Acknowledgement that the document has been filed

Land and Environment Court - Online Document Lodgement

[Lodge Documents] [Retrieve Documents] [Help] [Home] [Log out]

You are logged in as: Sally Kay

Your data was lodged successfully

Please click [PRINT](#) to print a copy of this page for your records. Note that this is optional.

The following document has been filed with the NSW Land and Environment Court: Lodgement number: 23
 Lodgement date: Wed 22 November 2000 15:52:43 GMT+11:00
 File number: 40042/2000
 Lodging solicitor: Sally Kay
 Email: sxk@lawsocnsw.asn.au
 Lodgement type: additional
 Lodged Document 0: Type=Affidavit
 Lodged Document 0: Reference=null
 Lodged Document 0: Supporting=false
 Lodged Document 0: FileDate=Wed 22 November 2000 15:52:43 GMT+11:00
 Lodged Document 1: Type=Notice of Discontinuance
 Lodged Document 1: Reference=null
 Lodged Document 1: Supporting=false
 Lodged Document 1: FileDate=Wed 22 November 2000 15:52:43 GMT+11:00
 Signer: c=AU,o=Demo Organisation,ou=Demo Unit,cn=Demo User
 Signing time(s): Wed 22 November 2000 14:52:42 GMT+11:00

5 Court Processing

5.1 Filing Overview

5.1.1 Processing

The documents to be lodged were divided into two groups.

Automatic this group of documents required no manual intervention in order to be accepted into the court file

Requiring Court Action this group of documents required an administrative function to be performed by a court officer before it could be accepted into the court file. For example, an initiating process required several tasks to be performed such as the allocation of a file number , applying a serve-by date and noting a return date.

The functions for the pilot were performed by a senior court officer who monitored the workflow and actioned all items requiring manual intervention. Generally these function were less troublesome than the manual acceptance of documents at the counter however the affixing of seals was not particularly efficient. This will be discussed in more detail below.

The original concept was for live matters to be run in parallel through the pilot but this proved impossible to achieve with the small number of participants and the short timeframe in which we were attempting to complete the lodgements. The time delay between the steps, such as serving documents on other parties, and the logistics of identifying the matters involving the participating solicitors was time consuming and deemed of little value to the processes being validated by the pilot.

The procedures initially required the Counter Clerk to check if an electronic file existed and contained an Application and a Notice of Appearance before accepting further documents. These business rules were not enforced during the pilot nor are they absolutely followed in the current manual system. This s because of the low business risk in accepting documents at face value at the counter. Documents filed in error are discovered later in the process, usually by the other party, and are easily corrected. This is also true of electronically lodged documents.

5.1.2 Serving of documents

The Court does not currently have responsibility for the distribution of material to the parties, that onus rests with the party filing the document. The Court is emphatic in its resolve not to distribute the material. How does a party lodging a document electronically then distribute the Court “stamped” copy to the other party?. The Pilot addressed this by the affixing of a seal to an electronic document in PDF format which the lodging party is able to download via the web interface and then serve the “paper” copy of the document. The recipient may accept the “paper” version or access the court file via the web interface to download the document itself (subject to having already lodged a Notice of Appearance). With the Court file being available online it is possible for the parties to distribute amongst themselves via emails advising of the event of lodgement. The pilot demonstrated that this technology could be successful although it did not attempt to define all the business rules for security and access that a production system would require.

5.1.3 Document Management

The Court does not have an adequate document management system to process documents being electronically filed. The Case Management system currently employed was not suitable for interfacing with the pilot project because the pilot needed a basic workflow system. A basic file management system was built for the pilot and incorporated the use of emails to facilitate the workflow requirements. The system generated emails on certain events to either confirm to participants an event had been registered or to prompt the court that an action was pending. Although simplistic in operation the email system was effective in ensuring tasks could be handled in an effective manner.

5.1.4 Audit Logs

The Court is the final arbitrator on whether or not a document has been lodged and the system maintained an audit log with each transaction of the events that had occurred. As all the transactions with the parties were secure the audit log provided a high level of assurance for authenticity. The use of PKI with the lodgements delivered a high level of confidence in total integrity of the system and the audit records included the storage of original encrypted transmissions. It was therefore possible to reconstruct the chain of events in any matter although the pilot did not automate this function. It would be important for a production system to have more analytical facilities.

5.1.5 Court Fees

The Department had technology being used by Registry Of Births, Deaths & Marriages for processing credit card payments and this was utilised to pilot the payment of fees. The current court rules do not facilitate payment of fees by other than cash or a solicitor's trust fund cheque. In an attempt to initiate further deliberations and to prove a concept of payments with electronic lodgements the system provided the means to effect payment by credit card. The concept of payments being processed before acceptance of a lodgement was proven and it would be a simple matter to implement the technology in a production environment. Credit Cards are not necessarily an ideal payment method for these transactions and direct debit or accounts should be explored further for court transactions.

5.1.6 E-Documents

The solicitors were required to complete an online web form to lodge a document. This enabled some structure to be applied to the communication in the form of identified metadata which described the document being lodged. This technique was very effective from the courts perspective as it facilitated the automation of workflow. If the form was erroneous in some way the subsequent processes would identify the problem and it could then be corrected. For example, it was possible to describe a court document in the form as an affidavit but the attached document was a photo of the kids. A glaring error such as this is not likely in the manual lodging at the counter however documents are usually accepted at face value and errors may occur. The vision for electronic lodgements probably lies in the integration of the lodgement process with the solicitors' systems providing direct output in a structured format such as XML.

5.2 Court Processing

5.2.1 Court Administration

Some Class 4 documents require manual processing by the court. When these documents were lodged electronically, an automatic email was sent to the LEC Court clerk, who was required to do the following:

- * Add metadata information to the lodgement system: the file number, serve by date and return date.
- * Download and open the document using Microsoft Word
- * Convert the document to PDF

- * Seal document if required (using Adobe Acrobat)
- * Upload the sealed document to the Court file

To achieve this task the court clerk chose the administration option and was presented with a list of the documents awaiting court action. Each document should then be processed.

Documents requiring court action				
Select	Document	File Number	Date Lodged	Lodgement #
<input type="radio"/>	Notice of Motion	10000/2000	2000-05-31	4
<input type="radio"/>	Subpoena to Give Evidence - (Seeking Abridgement)	10001/2000	2000-05-31	7

The next screen will display the form for entering court details. If a court seal is required, the document needs to be downloaded and further action taken to apply the seal.

Court Administration

Court Action for File Number: null - Application

[\[Click here to download document\]](#)

Enter required details for: unassigned - Application	
Enter new file number:	<input type="text"/> (format nnnn/yyyy)
Enter 'serve by' date:	<input type="text"/> (format dd/mm/yyyy)
Enter return date:	<input type="text"/> (format dd/mm/yyyy)
File to be uploaded:	<input type="text"/> <input type="button" value="Browse..."/>
<input type="button" value="<<< Back"/>	

5.2.2 Court Seal

The court clerk transforms the incoming document to a PDF format to apply the seal and to lodge the updated form into the court file. The seal used for the pilot was designed to replicate the stamp currently used. This was chosen to keep the new environment as familiar as possible to that currently used so that movement of matters between parties would be consistent no matter the media used.



5.3 Common Metadata

All documents lodged have the following data identified. Some of the metadata was entered during the lodgement process by the solicitor and much is added by the system from the defaults established for and by the individual solicitors.

- * Court file number
- * Applicant's name
- * Additional applicants' names
- * Respondent's name
- * Additional respondents' names
- * Solicitor on record
- * Firm name
- * Firm address
- * Firm DX
- * Firm phone
- * Firm fax
- * Contact email
- * Document type
- * Solicitor on record's reference
- * Filed on behalf of (ie either Applicant or Respondent)

5.3.1 Additional Metadata required for subpoenas

1. Seeking abridgement (Y/N) (if so, need to prompt to attach affidavit)
2. Return date

5.4 Payment Processing

Payment processing was an automated function and therefore the court clerk had no process in dealing with payments. Fees for the transactions used in the pilot could all be calculated according to certain criteria and the appropriate fees advised at data entry time by solicitor who authorised payment. The court file is noted as “fees paid” and the financial transaction is then able to be passed through to the appropriate accounting system.

The Pilot did not process live payments but simulated payments by the use of credit cards using the production system implemented for the Registry of Births Deaths & Marriages.

5.5 Document flow

(The step in brackets and italicised refers to cases where this is the first document received electronically in an existing matter)

Name of document	Fee	Court action	Notes
Application Class 4	\$531	<ol style="list-style-type: none"> 1. Allocate court file number 2. Allocate a 'serve by' date 3. Allocate a return date 4. Sign and seal completed document in PDF format. 5. Upload document to court file <p>An email will then be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.</p>	<ul style="list-style-type: none"> • Application comes with an Affidavit of Support • Only store completed document, that is document that has the additional material added by the court. • Only the party filing this document has access to the Court file at this stage • Requires a seal
Notice of Appearance		<ul style="list-style-type: none"> • Enable that party's Solicitor's access to the Court file • An email will be automatically generated advising the lodging party that the Notice has been filed 	
Subpoena for Production and to Give Evidence		<ol style="list-style-type: none"> 1. Is there a request for abridgement? If so, Court clerk has to notify Registrar. 2. Allocate return date 	<ul style="list-style-type: none"> • Additional metatags – “Seeking abridgement.” If this is checked, the Solicitor must also attach an Affidavit in support which the Registrar must see. Also “return date” • Requires a seal

Name of document	Fee	Court action	Notes
		<p>3. Sign and seal completed document in PDF format.</p> <p>4. Upload document to court file</p> <p>An email will then be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.</p> <p>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</p>	
<p>Subpoena for Production</p>	<p>\$48</p>	<p>1. Is there a request for abridgement? If so, Court clerk has to notify Registrar.</p> <p>2. Allocate return date</p> <p>3. Sign and seal completed document in PDF format.</p> <p>4. Upload document to court file</p> <p>An email will then be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.</p> <p><i>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i></p>	<ul style="list-style-type: none"> • Additional metatags – “Seeking abridgement.” If this is checked, the Solicitor must also attach an Affidavit in support which the Registrar must see. Also “return date” • Requires a seal
<p>Subpoena to Give Evidence</p>	<p>\$23</p>	<p>1. Is there a request for abridgement? If so, Court clerk has to notify Registrar.</p> <p>2. Allocate return date</p>	<ul style="list-style-type: none"> • Additional metatags – “Seeking abridgement.” If this is checked, the Solicitor must also attach an Affidavit in support which the Registrar must see. Also “return date”

Name of document	Fee	Court action	Notes
		<p>3. Sign and seal completed document in PDF format.</p> <p>4. Upload document to court file</p> <p>An email will then be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.</p> <p><i>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i></p>	<ul style="list-style-type: none"> • Requires a seal
Notice of Motion		<ol style="list-style-type: none"> 1. Allocate a hearing date 2. Sign completed document in PDF format. 3. Upload document to court file <p>An email will then be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.</p> <p><i>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i></p>	<ul style="list-style-type: none"> • No seal • Allocate date for service of N of M which is 3 clear days before the N of M is heard
Orders		<p>Sign and seal completed document in PDF format.</p> <p>An email will then be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.</p> <p><i>(If first electronic document received, Clerk checks</i></p>	<ul style="list-style-type: none"> • Requires seal

Name of document	Fee	Court action	Notes
		<i>hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i>	
Notice to Produce		None <i>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i>	<ul style="list-style-type: none"> An email will be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.
Affidavit		None <i>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i>	<ul style="list-style-type: none"> An email will be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.
Notice of Discontinuance		None <i>(If first electronic document received, Clerk checks hard copy file and activates access to the electronic file for the Solicitors for all parties where those Solicitors are part of the Pilot.)</i>	<ul style="list-style-type: none"> An email will be automatically generated which will be sent to the Solicitor filing the matter advising them that it has been filed.

6 Appendix – PKI

6.1 What is a PKI?

PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

- * Confidentiality - to keep information private
- * Integrity - to prove that information has not changed or been tampered with
- * Authentication - to prove the identity of an individual or application
- * Non-repudiation - to ensure that information cannot be disowned

6.2 The Components of a PKI

A Public Key Infrastructure is a combination of hardware and software products, policies and procedures. It provides the basic security required to carry out electronic business so that users, who do not know each other, or are widely distributed, can communicate securely through a chain of trust. PKI is based on digital IDs known as “digital certificates” which act like ‘electronic passports’, and bind the user’s digital signature to his or her public key.

There are five main components of PKI. These are:

- * Certification Authorities (CAs) – who issue and revoke public key certificates;
- * Registration Authorities (RAs) – who assure the binding between public keys and certificate holder identities and attributes;
- * Certificate holders (subscribers) – the party(s) to whom the certificates are issued and who can digitally sign and encrypt documents with those certificates;
- * Clients (relying parties) – who validate digital signatures and their certification paths from a known public key of a trusted CA;
- * Repositories – which store and make available certificates and Certificate Revocation Lists (CRLs).

6.2.1 Certification Authority (CA)

The CA system is the trust basis of a PKI as it manages public key certificates for their whole life cycle. The CA will:

- * Issue certificates by binding the identity of a user or system to a public key with a digital signature
- * Schedule expiry dates for certificates
- * Ensure certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs)

When implementing a PKI, an organization can either operate its own CA system, or use the CA service of a Commercial CA or Trusted Third Party.

Certificates can be distributed in a number of ways depending on the structure of the PKI environment, for example, by the users themselves, or through a directory service. A directory server may already exist within an organization or one may be supplied as part of the PKI solution.

6.2.2 *Registration Authority (RA)*

An RA provides the interface between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.

6.2.3 *Security Policy*

A security policy sets out and defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically it will include statements on how the organization will handle keys and valuable information, and will set the level of control required to match the levels of risk.

Certificate Practice Statement (CPS) - Some PKI systems are operated by Commercial Certificate Authorities (CCAs) or Trusted Third Parties, and therefore require a CPS. This is a detailed document containing the operational procedures on how the security policy will be enforced and supported in practice. It typically includes definitions on how the CAs are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users.

6.2.4 *PKI Applications*

A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits. Examples of applications are:

- * Communications between web servers and browsers
- * E-mail
- * Electronic Data Interchange (EDI)
- * Credit card transactions over the Internet
- * Virtual Private Networks (VPNs)

6.3 **PKI Operations**

The main operations of PKI are:

- * **Registration:** the process where a party makes themselves known to the CA (directly or through an RA);
- * **Initiation:** when the party gets the values needed to begin communicating with the PKI;
- * **Certification:** the process in which a CA issues the certificate for a party's public key and returns the certificate to the party or posts that certificate in a repository;
- * **Cross certification:** a cross-certification is a public key certificate issued by one CA to another CA which contains a public CA key associated with the private CA signature key. It is used to allow certain client systems or end entities in one administrative domain to communicate securely with client systems or end users in another domain;

- * **Key generation:** the key pairs can be generated by the party in their local environment or generated by the CA;
- * **Key update:** all key pairs need to be updated regularly and new keys issued when a key has passed its maximum lifespan or when a key has been compromised and must be replaced;
- * **Key expiry:** PKI needs to provide a facility to easily transition from a public key certificate with an existing key to a new public key certificate with a new key;
- * **Key compromise:** Encryption keys must not be disclosed. If they are revealed, the security offered by their encryption algorithm is compromised.
- * **Key pair recovery:** to prevent the total loss of the key – the private key can be backed up or stored by the CA;
- * **Revocation:** a public key certificate is expected to be used for its entire validity period; and
- * **Certificate Revocation Lists (CRLs)** - publicized data that is maintained by CAs allows parties relying on a digital signature certificate to check the validity of a certificate that has been tendered to them by subscribers.

6.4 Evaluating a PKI

6.4.1 Flexibility

It is essential that all components of a PKI are inter-operable, as it is unlikely that they will all be sourced from a single supplier. For example, the CA may have to interface with existing systems, such as directory servers already installed in the organization. The PKI should use open, standard interfaces such as LDAP and X.500(DAP), in order to ensure that it is capable of working with all standards-compliant directory servers.

In addition, many organizations have preferred suppliers of smart cards and hardware security modules (HSMs). Again, by using open, standard interfaces such as PKCS#11 (Cryptoki), the PKI has the flexibility to work with a wide range of security tokens.

In many PKI systems, face-to-face registration is required to provide the necessary level of trust. However, this may not always be appropriate, so remote registration may be required. The PKI should allow users to request certificates by e-mail, by using a standard web browser or automatically via network communication devices for VPNs.

For some large-scale implementations, certificates need to be automatically created in batches - for example for bankcards or national identity cards. In such instances, the PKI requires the flexibility of an automated RA process linked to the card database.

6.4.2 Ease of Use

Although the principles upon which a PKI system works can be complicated, the management should not be. The PKI must enable non-technical personnel, such as business administrators, to operate it with confidence. These operators should not have to deal with the intricacies of cryptographic algorithms, keys and signatures. It should be as easy as clicking on icons and letting the software application do the rest. The interface should be graphical and intuitive, assisting the management task, rather than obscuring it in complex database records. Flexibility and ease of use will seriously impact the return on investment in a PKI system as they affect issues such as training, maintenance, system configuration, integration and of course future growth in user numbers. These issues can make the cost of ownership of a PKI far higher than the initial implementation cost and therefore need to be considered in the evaluation phase.

6.4.3 Support for an Organization's Security Policy

PKI is becoming central to organizational security infrastructures, and any CA must be capable of reflecting and implementing the organization's security policy. A policy-driven PKI system therefore is critical in order to ensure that the certificate management process accurately reflects the roles of the CA and RA Operators and certificate users. For example, the CA Operator may decide to delegate the end-user certificate revocation to the RA Operators, whilst retaining revocation rights over RA Operator certificates.

6.4.4 Scalability

As an organization's use and reliance on PKI increases, it is essential that the PKI system can scale to match this growth. Initially, a PKI may only support a single application, however, it should be versatile enough to support further applications as they come on-line.

It should also be possible to add extra CA and RA components to support an increasing number of certificates as the PKI grows. In addition, a variety of certificate types and registration mechanisms may be needed as the scope of the PKI expands to include new services.

6.4.5 Interoperability

PKI is still in development stage and it is difficult to predict with any certainty the future uses and requirements for PKI systems. Standards for PKI are still evolving and in some cases are non-existent. Therefore, in order to protect your investment and prevent future interoperability headaches, it is vital to source a PKI that is completely open, and built to the most common and advanced commercial standards. This needs to be considered at the design stage, to ensure the seamless integration with the rest of your IT infrastructure.

6.4.6 The Security of the CA/RA

The CA/RA systems are at the heart of any PKI. The security of these systems is of primary importance, and if compromised, the whole PKI solution will be jeopardized.

In particular, the PKI must ensure the following:

- * The CA's private key should be held in a tamper-resistant security module and provision made for back-up copies for disaster recovery purposes.
- * Access to the CA and RA should be tightly controlled, eg using smart cards to ensure strong user authentication.
- * It should also be possible to configure the certificate management process such that more than one operator is required to authorize certification requests.
- * All certificate requests should be digitally signed by strong cryptographic authentication to detect and prevent hackers from deliberately generating bogus certificates.
- * All significant events performed by the CA/RA system should be recorded in a secure audit trail, where each entry is time/date stamped and signed, to ensure that entries cannot be falsified.
- * The CA should be approved and verified by an independent body, for example at least to ITSEC E2, but preferably to ITSEC E3 (Information Technology Security Evaluation Criteria). ITSEC is a recognized global standard for the measurement of security products and the E3 evaluation represents the highest level of commercial security sought today.

6.5 Secure Messaging

In traditional systems, a person's signature is the main identifier that provides authentication, integrity and non-repudiation. By providing the *digital equivalent* of a signature, we can provide the same security services electronically.

To create digital signatures we use cryptography. Cryptography involves using complex mathematical algorithms to transform data from one form into another form using an encryption key. In its new form, the data can only be understood when it is converted back into a readable form with a particular key.

6.5.1 Using digital signatures for integrity and authentication

We can provide integrity and authentication on messages by creating what is known as a digital signature. To create a signature, the sender must:

- * Put their message through a one-way 'hash function' to create a 'hash value'—a fixed-length string of data that represents the content of the message.
- * Encrypt this hash value using an encryption key. This creates their digital signature.
- * Attach the signature to the message.

When the recipient gets the message they:

- * Use a key to decrypt the digital signature, producing a hash value.
- * Put the message through the same hash function that the sender used to create a hash value.
- * Compare the hash value they have re-created with the hash value they decrypted from the digital signature.

If the hash value the recipient re-creates matches the hash value sent with the message, they know that no one has tampered with the message. If anyone has made even the tiniest change in the message, the hash value the recipient re-creates will be different. By using the key that belongs to the sender to decrypt the signature, the recipient knows that the message could only have been 'signed' by the key holder. If someone else signed it, the signature would not decrypt properly. This is how a digital signature provides integrity and authentication.

6.5.2 Using digital signatures for non-repudiation

In a symmetric key system the sender and the recipient both have the same encryption key, but this method only provides two of our security services: authentication and integrity. It does not provide non-repudiation because either party could have created the message.

To provide non-repudiation as well we have to use asymmetric encryption. Asymmetric encryption algorithms use a pair of different keys: a Public Key and a Private key.

A signature created with the Private key can only be decrypted with the corresponding Public key from that pair. To guarantee the security of the key pair, the owner of the Private key must keep it a secret, while their Public Key is made available publicly. This is unlike in a symmetric system where both sender and recipient must have the private key.

This means that only the owner of the Private key can sign messages using that key, but anyone who has their corresponding Public key can decrypt their signature. This provides integrity and authentication.

Because the sender used a Private key known only to them to encrypt the hash value, they can't deny having signed the message because no one else can create that signature. This provides non-repudiation.

6.5.3 *Using encryption for confidentiality*

The only way to make the message itself confidential is to encrypt the whole message, rather than just providing a digital signature. Encrypting the message transforms it into a coded form that can only be deciphered with the correct key and is the same as writing a letter in a code that only the receiver can decode.

Symmetric and asymmetric keys can both encrypt messages to provide confidentiality, but an asymmetric encryption system can encrypt a message with the recipient's Public key, knowing that only the correct recipient can decrypt the message with the corresponding Private key.

6.6 References

- Adams, C. and Lloyd, S. 1999. Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations. Indianapolis, IN: Macmillan Technical Publishing.
- Austin, Tom. 2001. PKI: A Wiley Tech Brief. New York, NY: John Wiley & Sons.
- Black, U. 2000. Internet Security Protocols: Protecting IP Traffic. Upper Saddle River, NJ: Prentice Hall PTR.
- Brands, S. 2000. Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. Cambridge, MA: MIT Press.
- Brands, S. 2000. Private Credentials. Zero Knowledge Systems Inc.
<http://www.zeroknowledge.com/media/credsnew.pdf>
- Feghhi, J., Feghhi, J. and Williams, P. 1999. Digital Certificates: Applied Internet Security. Reading, MA: Addison-Wesley.
- Jaworski, J. and Perrone, P. 2000. Java Security Handbook. Indianapolis, IN: Sams Publishing.
- Knudsen, J. 1998. Java Cryptography. Sebastopol, CA: O'Reilly & Associates, Inc.
- Scambray, J., McClure, S. and Kurtz, G. 2001. Hacking Exposed: Secrets & Solutions, Second Edition. Berkeley, CA: Osborne/McGraw-Hill.
- Schneier, B. 1996. Applied Cryptography. New York, NY: John Wiley & Sons.
- Schneier, B. 2000. Secrets and Lies: Digital Security in a Networked World. New York, NY: John Wiley & Sons.
- XML Standards Development Project: Electronic Court Filing Proposed Standard. 2000. Legal XML.
[http://www.courtxml.org/xml/JntXmlStandard.nsf/516c7664fda1528a862565ec00504473/9cbe71496cde5a14862567e100533da8/\\$FILE/LegalXMLCourtFilingProposedStandard.PDF](http://www.courtxml.org/xml/JntXmlStandard.nsf/516c7664fda1528a862565ec00504473/9cbe71496cde5a14862567e100533da8/$FILE/LegalXMLCourtFilingProposedStandard.PDF)
- Land Title Office spearheads electronic filing project. 1999. The Law Society of British Columbia.
http://www.lsbcc.org/library/bulletin/body_resource_bulletin-99-02.html#LTP electronic filing

7 Appendix – Technical Details

7.1 Baltimore Technologies FormSecure 4.2

7.1.1 Standards Support

- * X.509 v3 Public Key certificates.
- * S/MIME v2
- * X.500 LDAP v3 certificate directories.
- * 1024-bit RSA and 2048-bit RSA.
- * DES and Triple-DES.
- * SHA-1 and MD5.
- * FTP; SMTP; TCP/IP; HTTP
- * PKCS #11
- * Java 1.1 & 1.2
- * HTML.
- * TCP/IP, HTTP, Java, HTML.

7.1.2 Browsers Supported

- * Microsoft Internet Explorer v4
- * Netscape Navigator v4
- * Netscape Communicator v4.5

7.1.3 LDAP Directory Servers Supported

- * LDAP Netscape V3.
- * LDAP Critical Path InJoin 3

7.1.4 Certificate Support

FormSecure operates with X.509 class 1 certificates, for example:

- * Certificates generated with UniCERT.
- * Self-signed certificates generate with the FormSecure Certificate Wizard.
- * Any CA that issues standards-compliant X.509 certificates

7.1.5 Key Support

FormSecure operates with standard PKCS#12 keys (.p12 files), for example:

- * Keys generated with UniCERT and transported as .p12 (PKCS#12) files.
- * Self-generated keys using the FormSecure Certificate Wizard.
- * Any CA that generates standards-compliant PKCS#12 keys.

7.1.6 FormSecure Components Client Applets

- * Sign
- * Secure
- * Multi sign
- * Verify
- * Signed response
- * Smart card
- * De-Secure
- * Link to CA
- * OCSP Support
- * Control settings

7.1.7 System Requirements

FormSecure Client or FormSecure Toolkit applets:

- * Windows 95 (Service Pack 1plus Y2K patches), Windows 98 or Windows NT4 (SP3 plus Y2K patches)
- * Internet Explorer 4.x, Netscape Navigator 4.06+, and Netscape Communicator 4.5 or later
- * An Internet connection, e.g. via dial-up modem

Web server(s)

- * At least one transaction server to receive end-user data – a 300 MHz Pentium processor with 128 Mbytes of RAM is recommended as a minimum hardware platform
- * Windows NT4 Service Pack 3 plus Y2K patches or Unix
- * Microsoft IIS 4.0 Web Server plus a Java Servlet Manager. Baltimore provide ServletExec 2.2 from New Atlanta communications; or
- * Netscape Web Server; or
- * Apache Web Server
- * An on-line Internet connection

7.1.8 Security Operations

FormSecure secures end-user Web data by:

- * Signing it, or
- * Signing and encrypting it

FormSecure also provides the choice of the following encryption and signing algorithms:

- * Data encryption – DES or Triple DES encryption algorithm
- * Digital signature – MD5 or SHA-1 hashing algorithm

For strong confidentiality, authenticity and non-repudiation, Baltimore recommends using Triple DES and SHA-1.

7.2 Baltimore Technologies FormSecure Toolkit

Baltimore Technologies' FormSecure Toolkit provides a sub-set of features found in the FormSecure product. However, it provides complete programmatic control over the server-side application. The toolkit provides the following functionality:

- * Register for keys and certificates by either:
 - * Generating keys on the end-user machine and submit a certificate request and later retrieve signed certificate
 - * Importing keys and certificates generated by an RA
- * Sign data at the end-user machine
- * Verify data at the server
- * Change passphrase protecting the end-user's private key

The toolkit only provides single digital signature functions. Thus it does not provide any encryption capabilities. The Toolkit option provides three separate applets for registration, signing and administration together with a server API:

- * Sign Applet: Signs data with X.509 digital certificates
- * Registration Applet: Sends a PKCS#10 certificate request to CA
- * Administration Applet: Enables import of certificates in p12 files and changes of passphrase

The client applets are small and are designed to work on a variety of platforms. They are customisable from within an HTML page. The server Java 1.2 API handles server end registration and end-user data verification.

7.3 Database Design

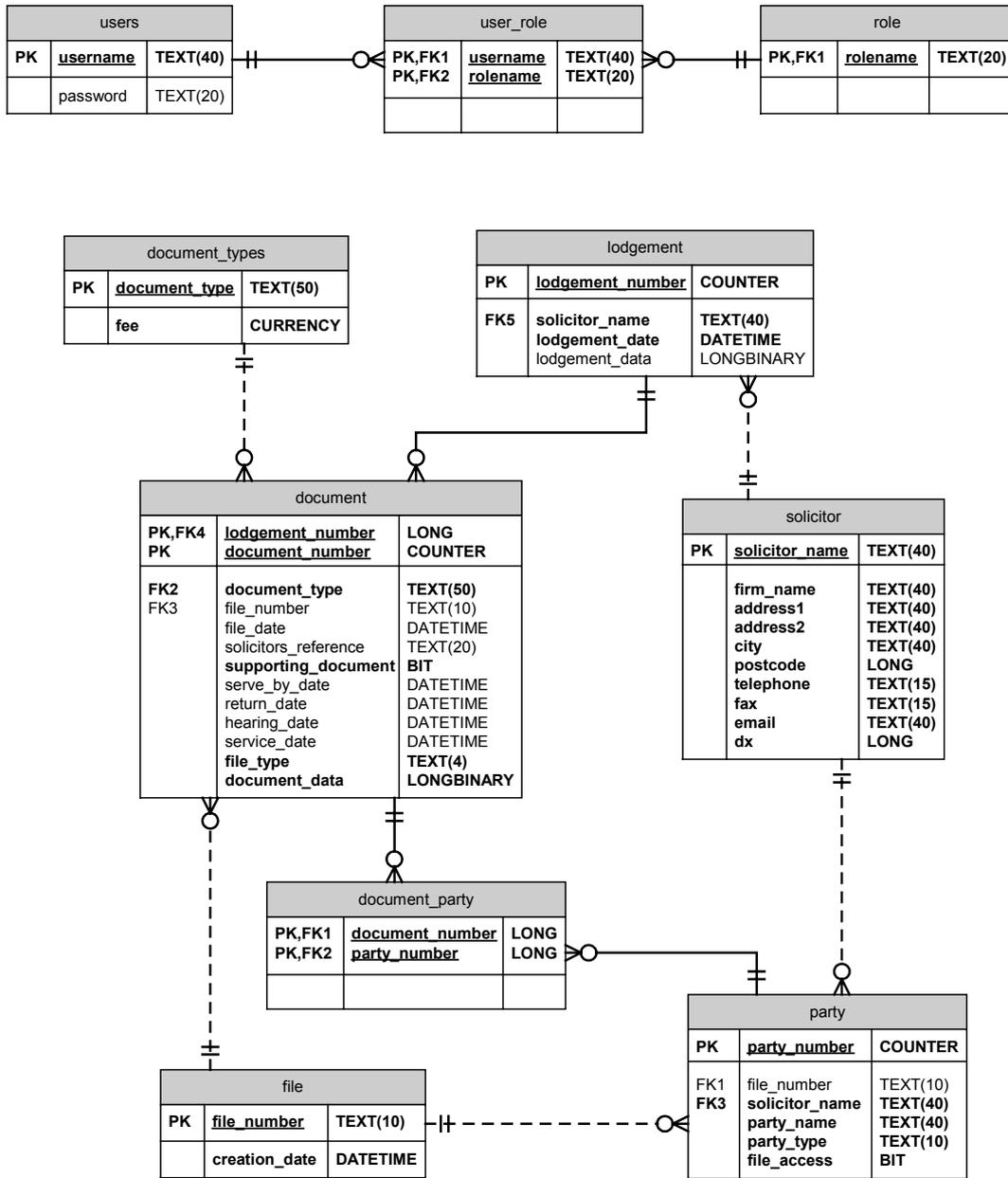


Figure – Entity-Relationship Diagram for simple Embedded Document Database

8 Glossary

3DES

See *DES*.

Authentication

A guarantee that web data really has come from the person who claims to have sent it. In the traditional mail system, a signature and a letterhead or watermark provide authentication.

Certificate

A block of data containing your public key and basic identification details, signed with the Certification Authority's private key to verify that it is authentic.

Certificate Fingerprint

A block of data that uniquely identifies a certificate.

Certificate Policy Statement

A document issued by a Certification Authority that prescribes the policies under which that authority issues public key certificates.

Certification Authority

A trusted third party that registers users and certifies their identities by signing their public key Certificate.

Confidentiality

The certainty that no-one has read data while it is en-route to you. In the traditional mail system a message is placed in a sealed envelope to provide this assurance.

Cryptography

Converting information into cipher or code, with a secret key that descrambles the message when it is received.

DES

This stands for Data Encryption Standard and is an industry-recognized method of encrypting data. There are two versions of this standard — "DES" for single DES and "3DES" for triple DES. Single DES is the original method used to encrypt data under this standard. Triple DES is a newer method and is more secure, but takes longer to encrypt — this will only be of concern if you are encrypting a large amount of data.

Desecured File

A file that has been authenticated and de-encrypted.

Desecured web data

Web data that has been authenticated, or authenticated and decrypted.

Digest

A sequence of alphanumeric characters created by passing web data through a 'hashing' algorithm. See *Hashing algorithm*. The MD5 hashing algorithm produces a 32-character sequence (see *MD5*), while the more secure SHA-1 hashing algorithm produces a 40-character sequence (see *SHA-1*).

Digital signature

A block of data created by hashing web data, then encrypting the resulting message digest using the sender's private signing key. See also *Digest* and *Signed file*.

A digital signature is verified by:

- decrypting the message digest using the sender's signing certificate.
- producing a new message digest, using the same hashing algorithm (see *Hashing algorithm*).
- comparing the two digests — if they agree, the message has not been changed in transit (see *Integrity*) and could only have been sent by the sender (see *Non-repudiation*).—

End user keys and certificates

An end user needs keys and certificates to use the PKI. These are obtained during end user registration.

An end user's keys and certificates are valid for a nominated period only, and typically expire after one year.

End user web pages

End user web pages contain "electronic forms" and are used for the entry and transmission of web data. Data entered into these pages is secured and sent to the web server.

Fingerprint

See *Digital signature* and *Certificate fingerprint*.

Hashing algorithm

An algorithm used to create a digest of the data (see *Digest*). The digest is used to prove the data has not been changed by a third party while in transit. The digest is then encrypted using the sender's private signing key and acts as a "digital signature", see *Non-repudiation*.

Two examples are the MD5 and SHA-1 hashing algorithms, see *MD5* and *SHA-1*.

HTML

Hypertext Markup Language, used in the design of web pages.

HTTP

HTTP stands for Hypertext Transfer Protocol. It is the network protocol used to deliver virtually all files and other data (collectively called *resources*) on the World Wide Web, whether they're HTML files, image files, query results, or anything else.

Integrity

Proof that web data has not been deliberately or accidentally altered during transmission, by comparing the digest sent with the message (see *Digest*) with a new digest produced from the message, using the same hashing algorithm (see *Hashing algorithm*).

In the traditional mail system, a sealed and undamaged envelope provides this evidence.

ISP

Internet Service Provider, a commercial agent providing web server (Internet storage and distribution) facilities.

MD5

This stands for Message Digest #5. It is an industry-recognized hashing algorithm, see *Hashing algorithm*.

Non-repudiation

The certainty of knowing that end users cannot later deny having sent web data, by verifying their digital signature, see *Digital signature*.

In the traditional mail system, the sender's signature proves this.

Passphrase

Used to ensure that an end user's private keys are made available only to the intended end user.

Private key

A cryptographic key kept secret, that enables you to:

- decrypt web data that has been encrypted using your public key.
- digitally sign web data.

Your end users' private keys allow them to digitally sign the web data they send you.

Public key Certificate

A Certificate issued by a Certification Authority containing a person or organizations' name and position, their public authenticity key and public confidentiality key, and other information such as the Certificate's expiry date.

Public key Certificates are distributed throughout a Public key system to allow people to encrypt messages for transmission (using the receiver's public confidentiality key) and to decrypt the digital signature in received messages (using the sender's public authenticity key).

Public key system

A cryptographic system that uses two keys:

- a *public key*, known to everyone, that is used to encrypt messages
- a *private* or *secret key*, known only to the recipient of a message, that is used to decrypt the message. It is virtually impossible to deduce a private key from a public key.

Public key systems are simple to use and extremely secure and are becoming popular for transmitting information via the Internet.

Registration Authority

A keys and certificates agency acting for a group of users in a Public key system. A registration authority:

- generates public and private keys
- requests Certification of public keys from a Certification Authority — this Certification is provided in the form of public key Certificates
- is required to comply with the policies of the Certification Authority it obtains Certificates from, including specific requirements for the verification of its users' identities

Registration Officer

The person who administers a registration authority. One of their prime responsibilities is entering new end user registration details.

RSA

RSA is an industry-recognized standard for session key generation and secure key exchange, see *Session Key*, named after its creators: Rivest, Shamir and Adleman.

FormSecure can use this standard in conjunction with :

- the DES or 3DES encryption algorithm —see *DES*) to encrypt and decrypt web data.
- the SHA-1 or MD5 hashing algorithm to encrypt and decrypt message digests —see *SHA-1*, *MD5*, *Hashing algorithm* and *Digest*).

Secured web data

Signed web data that has been encrypted by passing it through a complex mathematical process controlled by a number called a key.

Session Key

A session key is a private key that is generated for use in an Internet session. Session keys are used for data encryption and decryption.

SHA-1

This stands for Secure Hashing Algorithm #1. It is an industry-recognized hashing algorithm, see *Hashing algorithm*.

Signed file

A file that has been 'signed' by creating and encrypting a message digest of the file. A signed file is normally *secured* before it is sent to a recipient, see *Secured web data*.

SMTP

SMTP stands for Simple Mail Transfer Protocol, a communications standard for sending e-mail messages. Most e-mail messages sent over the Internet use SMTP.

Transaction processing system

The system that processes end user transactions received on your transaction server.

Trust status

A trust status indicates the degree of confidence that can be placed in a certificate. There are four trust statuses; explicitly trusted, explicitly distrusted, inherited trust and unknown trust.

URL

Universal Resource Location, a standard for specifying the location of a local or remote HTTP web page or FTP file.

Web server

Web servers are processing sites for HTTP transactions. They provide access to web pages stored locally or remotely by receiving requests for these pages — including verifying the requestor's authority to access the page, if required — and transmitting the page to the requestor.

Web transaction

Any end user data that is sent over the Internet for transaction processing. The data may be sent as:

- a completed web page, using HTTP (this is the method used by FormSecure).
- a computer file, using FTP (Internet file transfer protocol) or SMTP (Internet e-mail).

Website

A storage location for web pages.